ЎЗБЕКИСТОН ДАВЛАТ СТАНДАРТИ

Ахборот технологияси

ХАВФСИЗЛИКНИ ТАЪМИНЛАШ МЕТОДЛАРИ

АХБОРОТ ХАВФСИЗЛИГИНИ БОШҚАРИШНИНГ АМАЛИЙ ҚОИДАЛАРИ

(ISO/IEC 27002:2005, IDT)

Расмий нашр

Ўзбекистон стандартлаштириш, метрология ва сертификатлаштириш агентлиги
Тошкент

Сўз боши

1 Ўзбекистон алоқа ва ахборотлаштириш агентлигининг Фан-техника ва маркетинг тадқиқотлари маркази томонидан ИШЛАБ ЧИҚИЛГАН

2 Ўзбекистон алоқа ва ахборотлаштириш агентлиги томонидан КИРИТИЛГАН

3 Ўзбекистон стандартлаштириш, метрология ва сертификат-лаштириш агентлигининг 27.11.2008 даги 05-129-сон қарори билан ҚАБУЛ ҚИЛИНГАН ВА АМАЛГА КИРИТИЛГАН

4 Ушбу стандарт ИСО/МЭК 27002:2005 «Ахборот технологияси. Хавфсизликни таъминлаш методлари. Ахборот хавфсизлигини бошқаришнинг амалий қоидалари». (ISO/IEC 27002:2005 «Information technology. Security techniques. Code of practice for security management») халқаро стандарти билан бир хил.

Мувофиқлик даражаси - бир хил (IDT)

5 БИРИНЧИ МАРТА КИРИТИЛГАН

Ушбу стандарт ва унга киритилган ўзгартишларни Ўзбекистон Республикаси ҳудудида амалга киритиш (амал қилишини тўхтатиш) тўғрисидаги ахборот «Ўзстандарт» агентлиги томонидан нашр этиладиган кўрсаткичда эълон қилинади

Ушбу стандартни Ўзбекистон Республикаси ҳудудида расман эълон қилишнинг мутлақ ҳуқуқи «Ўзстандарт» агентлигига тегишли

Мундарижа

Кириш

Ахборот хавфсизлиги нима?

Ахборот - бу бизнеснинг бошқа муҳим активлари каби қийматга эга бўлган актив ва шундай экан, у тегишли равишда муҳофаза қилинган бўлиши керак. Бу ўзаро алоқалар билан доимо ривожланаётган амалий иш муҳитида айниқса муҳим. Ҳозирги вақтда ушбу ўзаро алоқалар натижасида ахборот таҳдидлар ва заифликларнинг ўсиб бораётган сони ва турли хилига дучор бўлмоқда (Ахборот тизимлари ва ОЕСД тармоқларининг хавфсизлиги бўйича кўрсатмалар).

Ахборот турли шаклларда мавжуд бўлиши мумкин. У қоғоз ташувчида жойлаштирилган бўлиши, электрон кўринишда сақланиши, почта орқали ёки телекоммуникацияларнинг электрон воситаларидан фойдаланиб узатилиши, пленкадан намойиш қилиниши ёки оғзаки ифодаланиши мумкин. Ахборот мавжудлигининг шаклидан, уни тарқатиш ёки сақлаш усулидан қатъи назар у доим адекват муҳофазаланган бўлиши керак.

Ахборот хавфсизлиги - бу ахборотни бизнеснинг узлуксизлигини таъминлаш, бизнес хавфларини минимумга келтириш ва инвестицияларни қайтаришни ҳамда бизнес имкониятларини максимал ошириш масқсадида таҳдидларнинг кенг спектридан муҳофаза қилиш демакдир.

Ахборот хавфсизлигига дастурий таъминотнинг сиёсатлари, методлари, процедуралари, ташкилий тузилмалари ва дастурий таъминот функциялари томонидан тақдим этилиши мумкин бўлган ахборот хавфсизлигини бошқариш бўйича тадбирларнинг тегишли комплексини амалга ошириш йўли билан эришилади. Кўрсатилган тадбирлар ташкилотнинг ахборот хавфсизлиги мақсадларига эришишини таъминлаши керак.

Ахборот хавфсизлигининг зарурати

Ахборот ва уни сақлаб турувчи жараёнлар, ахборот тизимлари ва тармоқ инфратузилмаси бизнеснинг бебаҳо активлари бўлиб ҳисобланади. Ахборот хавфсилигини аниқлаш, таъминлаш, сақлаб туриш ва яхшилаш ташкилотнинг рақобатбардошлилиги, қадрлилиги, даромадлилиги, қонун ҳужжатларига мувофиқлигини ва ишбилармонлик обрўсини таъминлашда катта аҳамиятга эга.

Ташкилотлар, уларнинг ахборот тизимлари ва тармоқлар хавфсизликнинг турли компьютер фирибгарлиги, шпионлик, зараркунандалик, вандализм, ёнғинлар ёки сув тошқинлари каби таҳдидлар билан кўпроқ тўқнашмоқдалар. Зарарнинг бундай компьютер вируслари, компьютерни бузиб очиш ва «хизмат кўрсатишдан бош тортиш» туридаги ҳужумлар манбалари кенг тарқалмоқда, агрессивроқ бўлиб бормоқда ва кўпроқ маҳорат билан шаклланмоқда.

Ахборот хавфсизлиги бизнеснинг жамоат ва хусусий секторида, шунингдек критик инфратузилмаларни муҳофаза қилишда муҳим. Ахборот

хавфсизлиги иккала секторда ҳам ёрдам бериши керак, масалан электрон ҳукуматни ёки электрон бизнесни жорий қилишда тегишли хавфлардан мустасно бўлиш ёки уларни камайтириш учун. Умумий фойдаланишдаги тармоқларнинг ва хусусий тармоқларнинг биргаликда ишлаши, шунингдек, ахборот ресурсларидан биргаликда фойдаланиши ахборотдан фойдаланишни бошқаришни қийинлаштиради. Маълумотларга тақсимлаб ишлов беришдан фойдаланиш тенденцияси марказлаштирилган назорат самарадорлигини сусайтиради.

Кўпгина ахборот тизимларини лойиҳалаштиришда хавфсизлик масалалари эътиборга олинмас эди. Техник воситалар билан эришилиши мумкин бўлган хавфсизлик даражаси бир қатор чеклашларга эга бинобарин, тегишли бошқарув воситалари ва процедуралар билан таъминланиши керак. Ахборот хавфсизлигини бошқариш бўйича зарур тадбирларни танлаш пухталик билан режалаштириш ва деталлаштиришни талаб қилади.

Ахборот хавфсизлигини бошқариш, камида ташкилот барча ходимларининг иштирок этишига муҳтож. Шунингдек, етказиб берувчилар, мижозлар ёки акциядорларнинг иштирок этиши ҳам талаб қилиниши мумкин. Бундан ташқари, бегона ташкилот мутахассисларининг маслаҳатлари керак бўлиб қолиши мумкин.

Агар ахборот хавфсизлиги соҳасини бошқариш бўйича тадбирлар ахборот тизимини лойиҳалаштириш босқичида техник топшириққа киритилса, анча арзонга тушади ва самаралироқ бўлади.

Ахборот хавфсизлиги талабларини аниқлаш

Ташкилот ўзининг ахборот хавфсизлигига бўлган талабларини қуйидаги учта муҳим омилни ҳисобга олиб аниқлаши муҳим:

1) Биринчиси бизнеснинг глобал стратегияси ва ташкилотнинг мақсадларини эътиборга олиб, ташкилотда хавфларни аниқлашдан олинган. Хавфларни баҳолаш ёрдамида ташкилот активларига таҳдидлар аниқланади, тегишли активларнинг заифлиги ва таҳдидлар пайдо бўлиш эҳтимоли, шунингдек келиб чиқиши мумкин бўлган оқибатлар баҳоланади.

2) Ташкилот, унинг савдо шериклари, пудратчилар ва хизмат-ларни етказиб берувчилар, қониқтириши керак бўлган юридик талаблар, қонун ҳужжатларининг талаблари, тартибга солувчи ва шартномавий талаблар, шунингдек, ушбу томонларинг ижтимоий маданий муҳити бошқа омил бўлиб ҳисобланади.

3) Ўзининг ишлашини таъминлаш учун ташкилот томонидан ишлаб чиқарилган принциплар, мақсадлар ва талабларнинг махсус тўплами яна бир омил бўлиб ҳисобланади.

Ахборот хавфсизлигининг хавфларини баҳолаш

Ахборот хавфсизлигига қўйиладиган талаблар хавфларни мунтазам баҳолаш ёрдамида аниқланади. Ахборот хавфсизлигини бошқариш бўйича тадбирларга кетган сарф-харажатлар ахборот хавфсизлигининг бузилиши

натижасида ташкилотга етказилиши мумкин бўлган зарар миқдорига пропорционал бўлиши керак.

Ушбу баҳолашнинг натижалари ахборот хавфсизлиги билан боғлиқ хавфларни бошқариш соҳасида аниқ чоралар ва устуворликларни белгилашга, шунингдек, ушбу хавфларни минимумга келтириш мақсадида ахборот хавфсизлигини бошқариш бўйича тадбирларни жорий қилишга ёрдам беради.

Мавжуд тадбирларнинг самарадорлилигига таъсир кўрсатиши мумкин бўлган ҳар қандай ўзгаришларни ҳисобга олиш учун хавфлар таҳлилини вақти-вақти билан такрорлаб туриш керак.

Хавфларни баҳолаш тўғрисидаги ахборотни (хавфсизлик хавфларни аниқлаш) 4.1-бандда топиш мумкин.

Ахборот хавфсизлигини бошқариш бўйича тадбирларни танлаш

Ахборот хавфсизлигига қўйиладиган талаблар белгиланганидан ва хавфлар аниқланганидан сўнг хавфларни қабул қилса бўладиган даражагача пасайишини таъминлайдиган, ахборот хавфсизлигини бошқариш бўйича тадбирларни танлаш ва жорий этиш керак. Ушбу тадбирлар ушбу стандартдан, бошқа манбалардан танлаб олиниши, шунингдек, ахборот хавфсизлигини бошқариш бўйича ташкилотнинг ўзига хос эҳтиёжларини қондирадиган тадбирлар ишлаб чиқилиши мумкин. Ахборот хавфсизлигини бошқариш бўйича тадбирларни танлаш хавфларни қабул қилиш мезонларига, хавфларга баҳо бериш вариантларига асосланган ташкилий қарорларга ва хавфларни ташкилотда қабул қилинган бошқаришга умумий ёндошишга боғлиқ. Ушбу танловни тенгишли миллий ва халқаро қонун ҳужжатлари ва нормалар билан мувофиқлаштириш керак.

Ушбу стандартда келтирилган ахборот хавфсизлигини бошқариш бўйича баъзи тадбирлар ахборот хавфсизлигини бошқариш учун амал қилинадиган принциплар сифатида қабул қилиниши ва кўпгина ташкилотлар учун қўлланиши мумкин. Бундай тадбирлар қуйироқда «Ахборот хавфсизлигини жорий қилиш учун таянч нуқта» сарлавҳаси остида батафсилроқ кўриб чиқилади.

Ахборот хавфсизлигини бошқариш бўйича тадбирлар ва хавфларни баҳолашнинг бошқа вариантларини танлаш бўйича ахборот «Хавфсизлик хавфларига ишлов бериш» 4.2-бандда жойлашган.

Ахборот хавфсизлигини жорий қилиш учун таянч нуқта

Ахборот хавфсизлигини бошқариш бўйича алоҳида тадбирлар ахборот хавфсизлигини бошқариш учун амал қилинадиган принциплар сифатида қабул қилиниши ва уни жорий қилиш учун таянч нуқта бўлиб хизмат қилиши мумкин. Бундай тадбирлар қонун ҳужжатларининг асосий

талабларига асосланади ёки ахборот хавфсизлиги соҳасида умумий қабул қилинган амалиёт сифатида қабул қилиниши мумкин.

Қонунчилик нуқтаи назаридан ахборот хавфсизлигини бошқариш бўйича асосий чоралар қуйидагилар ҳисобланади:

a) маълумотларни муҳофаза қилиш ва шахсий ахборотнинг конфиденциаллиги(15.1.4);

b) ташкилот ҳужжатларини муҳофаза қилиш (15.1.3);

c) интеллектуал мулкка эгалик қилиш ҳуқуқи (15.1.2);

Ахборот хавфсизлиги соҳасида умумий қабул қилинган амалиёт сифатида ҳисобланган ахборот хавфсизлигини бошқариш бўйича тадбирлар қуйидагиларни ўз ичига олади:

a) ахборот хавфсизлиги сиёсатини ҳужжатлаштириш (5.1.1);

b) ахборот хавфсизлигини таъминлаш бўйича мажбуриятларни тақсимлаш (6.1.3);

c) ахборот хавфсизлиги қоидаларига ўқитиш (8.2.2);

d) иловалардаги ахборотга тўғри ишлов бериш (12.2);

e) техник заифликларни бошқариш стратегияси(12.6);

f) ташкилотнинг узлуксиз ишини бошқариш (14):

g) ахборот хавфсизлиги инцидентлари ва такомиллаштиришларини бошқариш (13.2).

Санаб ўтилган тадбирларни кўпгина ташкилотлар ва ахборот муҳити учун қўлласа бўлади. Ушбу стандартда келтирилган барча тадбирлар муҳим ҳисобланса ҳам, қандайдир чоранинг ўринли бўлиши ташкилот тўқнаш келадиган муайян хавфлар нуқтаи назаридан белгиланиши керак. Демак, юқорида таърифланган ёндашиш ахборот хавфсизлигини таъминлаш бўйича тадбирларни жорий қилиш учун таянч нуқта бўлиб ҳисобланишига қарамай, у хавфларни баҳолашга асосланган ахборот хавфсизлигини бошқариш бўйича тадбирларни танлашнинг ўрнини босмайди.

Муваффақиятнинг энг муҳим омиллари

Тажриба шуни кўрсатадики, ташкилотда ахборот хавфсизлигини таъминлаш бўйича тадбирларни муваффақиятли жорий қилиш учун қуйидаги омиллар ҳал қилувчи ҳисобланади:

a) ахборот хавфсизлиги мақсадлари, сиёсатлари ва процедураларининг бизнес мақсадларига мувофиқлиги;

b) хавфсизлик тизимини жорий қилиш, қўллаб-қувватлаш, мониторингини ўтказиш ва модернизация қилишга ёндашишнинг корпоратив маданият билан мувофиқлиги;

c) раҳбарият томонидан реал қўллаб-қувватлаш ва манфаатдорлик;

d) хавфсизлик талабларини, хавфларни баҳолаш ва хавфларни бошқаришни аниқ тушуниш;

e) ташкилот раҳбарлари ва ходимлари томонидан ахборот хавфсизлигининг самарали маркетингини ўтказиш, шунингдек, ахборот хавфсизлигининг чораларини қўллаш заруратини тушунишни таъминлаш;

f) ахборот хавфсизлиги сиёсатига тегишли йўриқномалар, тавсияларни ва тегишли стандартларни барча ходимлар ва субпудратчиларга бериш;

q) ахборот хавфсизлигини бошқариш бўйича тадбирларни молиялаштириш шарти;

h) ўқитиш ва тайёрлашнинг зарур даражасини таъминлаш;

i) ахборот хавфсизлиги инцидентларини бошқаришнинг самарали жараёнини тасдиқлаш;

j) ўлчанадиган кўрсаткичларнинг[1] ахборот хавфсизлигини бошқаришнинг самарадорлилигини ва уни яхшилаш бўйича бажарувчилардан тушган таклифларни баҳолаш учун фойдаланиладиган ҳар томонлама ва балансланган тизими.

Ташкилотга тегишли қўлланмаларни ишлаб чиқиш

Ушбу стандарт ташкилотнинг муайян эҳтиёжлари учун қўлланмалар ишлаб чиқиш учун таянч нуқта сифатида баҳоланиши керак. Ушбу стандартда келтирилган йўриқномалар ва тадбирларнинг ҳаммаси ҳам қўллашга яроқли бўлавермайди.

Бундан ташқари, ушбу стандартга киритилмаган қўшимча чоралар керак бўлиб қолиши мумкин. Бу ҳолда аудиторлар ва бизнес бўйича шериклар томонидан ўтказиладиган мувофиқлик текширувини енгиллаштирадиган, бир вақтда бир неча томондан қилинган ҳаволаларнинг сақланиши фойдали бўлиши мумкин.

[1] Ахборот хавфсизлигининг кўрсаткичлари ушбу стандартни кўриб чиқиш соҳасига кирмайди

ЎЗБЕКИСТОН ДАВЛАТ СТАНДАРТИ

Ахборот технологияси

ХАВФСИЗЛИКНИ ТАЪМИНЛАШ МЕТОДЛАРИ

АХБОРОТ ХАВФСИЗЛИГИНИ БОШҚАРИШНИНГ АМАЛИЙ ҚОИДАЛАРИ

Информационная технология

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

ПРАКТИЧЕСКИЕ ПРАВИЛА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Information technology. Security techniques. Code of practice for information security management

Жорий этиш санаси 2008-12-01
Амал қилиш муддати чекланмаган

1 Қўллаш соҳаси

Ушбу стандарт ташкилотда ахборот хавфсизлигини бошқариш бўйича тавсияларни ўз ичига олади ва уни инициация қилиш, жорий этиш, қўллаб-қувватлаш ва яхшилаш бўйича умумий принципларни белгилайди. Ушбу стандартда таърифланган тавсиялар хавфларни аниқлашда белгиланадиган талабларни таъминлаш мақсадида жорий этиш учун мўлжалланган, улар ахборот хавфсизлигини бошқаришнинг умум қабул қилинган масалалари бўйича умумий бошқарувдан иборат.

Ушбу стандарт хавфсизлик стандартларини ишлаб чиқиш ва ташкилотда хавфсизликни бошқариш бўйича амалий тадбирларни танлаш учун, шунингдек, ташкилотлар ўртасида хизматга оид муносабатлар ишончини таъминлашда асос бўлади.

2 Атамалар ва таърифлар

Ушбу стандартда қуйидаги атамалар тегишли таърифлари билан қўлланилган:

2.1 актив: Ташкилот учун қимматли бўлган бирор нарса [ISO/IEC13335-1:2004]

2.2 бошқариш воситаси: Сиёсатлар, процедуралар, тавсиялар, тажрибалар ёки маъмурий, техник, бошқарув ёки юридик хусусиятга эга бўлиши мумкин бўлган ташкилий структураларни ўз ичига олган хавфни бошқариш воситалари.

Изоҳ - Бошқариш воситаси, шунингдек «хавфсизлик чоралари» ёки «қарши чоралар» учун синоним сифатида ишлатилади.

2.3 тавсия: [ISO/IEC13335-1:2004] сиёсатларида қўйилган мақсадларга эришиш учун нима ва қандай қилинган бўлиши кераклигини ойдинлаштирувчи таъриф.

2.4 ахборотга ишлов бериш воситалари: Ахборотга ишлов бериш бўйича исталган тизимлар, сервислар ёки инфратузилмалар, шунингдек, уларнинг физик жойи.

2.5 ахборот хавфсизлиги: Ахборотнинг конфиденциаллигини, бутлигини ва ундан эркин фойдалана олишликни таъминлаш; бундан ташқари ҳақиқийлик, кузатилиши мумкинлиги, аппеляциялаш мумкинлиги ва ишончлилик каби хусусиятлари киритилиши мумкин.

2.6 ахборот хавфсизлиги воқеалари: Ахборот хавфсизлиги сиёсатининг мумкин бўлган бузилиши ёки муҳофаза қилиш воситаларининг бузилишини кўрсатадиган тизим ёки тармоқ ҳолатининг идентификация қилинган ҳолати ёхуд [ISO/IEC TR 18044:2004] хавфсизлик учун катта аҳамиятга эга бўлган, олдиндан маълум бўлмаган вазият

2.7 ахборот хавфсизлиги инциденти: Ахборот хавфсизлигининг ягона воқеаси ёки бир қатор ноҳуш ёки кутилмаган воқеалари туфайли бизнес ахборотнинг компрометация қилиниш эҳтимоли ва ахборот хавфсизлигига [ISO/IEC TR18044:2004] таҳдидларнинг эҳтимоли катта бўлиши мумкин бўлган ягона воқеа ёки бир қатор ноҳуш ёки кутилмаган воқеалар.

2.8 сиёсат: Раҳбарият томонидан расман ифодаланган умумий мақсад ёки йўналиш.

2.9 хавф: Воқеа эҳтимоли ва унинг оқибатларининг бирлиги [ISO/IEC 73:2002 қўлланма].

2.10 хавфлар таҳлили: Хавф манбаларини аниқлаш ва уни ҳисоблаб чиқариш бўйича ахборотдан мунтазам фойдаланиш [ISO/IEC 73:2002 қўлланма].

2.11 хавфларни аниқлаш: Хавфларни таҳлил қилиш ва баҳолашни ўз ичига оладиган жараён [ISO/IEC 73:2002 қўлланма].

2.12 хавфларни баҳолаш: Хавф моҳиятини аниқлаш мақсадида бажариладиган, ҳисобланган хавф ва хавф мезонларини таққослаш жараёни [ISO/IEC 73:2002 қўлланма].

2.13 хавфларни бошқариш: Хавфга нисбатан ташкилотга раҳбарлик қилиш ва бошқариш бўйича мувофиқлаштирилган фаолият.

Изоҳ - Хавфларни бошқариш одатда хавфларни аниқлаш, хавфларга ишлов бериш, хавфларни қабул қилиш ва хавфлар тўғрисида хабар беришни ўз ичига олади [ISO/IEC 73:2002 қўлланма].

2.14 хавфларга ишлов бериш: Хавфни ўзгартириш бўйича тадбирларни танлаш ва жорий қилиш жараёни [ISO/IEC 73:2002 қўлланма].

2.15 учинчи томон: Кўриб чиқилаётган масалада қатнашадиган томонларга боғлиқ бўлмаган жисмоний ёки юридик шахс [ISO/IEC 72:1996 қўлланма].

2.16 таҳдид: Тизим ёки ташкилотга зарар келтириши мумкин бўлган ноҳуш инцидентнинг потенциал сабаби [ISO/IEC 13335-1:2004 қўлланма]**.**

2.17 заифлик: Битта ёки ундан кўп таҳдидларни амалга оширишда фойдаланилиши мумкин бўлган актив ёки активлар тўпламининг заиф жойи [ISO/IEC 13335-1:2024 қўлланма].

3 Ушбу стандарт структураси

Ушбу стандарт хавфсизликнинг 39 та асосий тоифасини, шунингдек «Хавфларни аниқлаш ва уларга ишлов бериш» кириш бўлимини ўз ичига олган ахборот хавфсизлигини бошқариш механизмларининг таърифига эга ўн битта асосий бўлимдан иборат**.**

3.1 Бўлимлар

Ҳар бир бўлим хавфсизликнинг бир неча асосий тоифаларини ўз ичига олади. Ҳужжат ўн битта бўлимдан иборат (қавсларда ҳар бир бўлимдаги хавфсизлик асосий тоифаларининг сони келтирилган):

a) Хавфсизлик сиёсати (1);

b) Ахборот хавфсизлигини таъминлашни ташкил қилиш (2);

c) Активларни бошқариш (2);

d) Ходимларнинг хавфсизлиги (3);

e) Жисмоний хавфсизлик ва атроф-муҳит хавфсизлиги (2);

f) Маълумотларни узатишни ва операцион процедураларни бошқариш (10);

g) Фойдаланишни бошқариш (7);

h) Ахборот тизимларини сотиб олиш, ишлаб чиқиш ва уларга хизмат кўрсатиш (6);

i) Ахборот хавафсизлиги инцидентларини бошқариш (2);

j) Ташкилот узлуксиз ишининг таъминланишини бошқариш (1);

k) Талабларга мувофиқлик.

Изоҳ - Ушбу стандарт бўлимларининг тартиби уларнинг муҳимлигини билдирмайди. Вазиятга кўра барча бўлимлар муҳим бўлиши мумкин, бинобарин, ушбу стандартни қўллайдиган ҳар бир ташкилот ўзи учун долзарб бўлимларни, уларнинг муҳимлигини ва алоҳида бизнес жараёнларда қўлланиши мумкинлигини аниқлаши керак. Шунингдек, ушбу стандартда барча рўйхатлар устуворлик тартибида жойлаштирилмаган, агар бу яққол кўрсатилмаган бўлса.

3.2 Хавфсизликнинг асосий тоифалари

Хавфсизликнинг ҳар бир асосий тоифаси қуйидагиларни ўз ичига олади:

a) нимага эришиш зарурлигини ифодаловчи бошқариш мақсади;

b) бошқариш мақсадига эришиш учун қўлланиши мумкин бўлган бошқаришнинг бир неча воситалари.

Бошқариш воситаларининг таърифи қуйидаги тарзда келтирилган:

Бошқариш воситаси

Қўйилган мақсадни қониқтириш учун бошқариш воситаларининг аниқ ифодаланишини белгилайди.

Жорий этиш бўйича қўлланма

Бошқариш воситасини жорий этиш ва қўйилган мақсадларга эришишга ёрдам бериш бўйича батафсил ахборотни тақдим этади. Баъзи ҳолларда, бошқариш воситаларини жорий этишнинг қабул қилса бўладиган усуллари учраганда қўлланмалар тўғри келмаслиги мумкин.

Бошқалар

Масалан юридик масалалар ва бошқа стандартларга ҳаволаларни кўриб чиқиш учун зарур бўлиши мумкин бўлган ахборот келтирилади.

4 Хавфларни аниқлаш ва уларга ишлов бериш

4.1 Хавфсизлик хавфларини аниқлаш

Хавфларни аниқлашда, хавфларни ташкилотга мос келадиган, қабул қилса бўладиган мезонлар ва мақсадлар бўйича ўлчаш ва устувор қўйиш керак. Хавфларни аниқлаш натижалари бўйича раҳбарият томонидан ахборот хавфсизлиги хавфларини бошқариш бўйича ва ушбу хавфлардан муҳофаза қилиш бўйича устувор хатти-ҳаракатлар белгиланган бўлиши керак.

Ташкилотнинг турли бўлинмаларини ёки алоҳида ахборот тизимларини қамраб олиш мақсадида хавфларни аниқлаш ва бошқариш воситаларини танлаш жараёнини бир неча марта бажариш талаб қилиниши мумкин.

Хавфларни аниқлашда тизимли ёндошишни қўллаш тавсия этилади. Бу хавфларни баҳолаш ва таҳлил қилишни аниқлашда, шунингдек хавфларни хавфлар мезонлари билан таққослаш жараёнида зарурдир.

Хавфларни аниқлашни хавфсизлик талабларига ва хавфли вазиятларга ўзгартиришлар киритиш учун вақти-вақти билан такрорлаб туриш керак, масалан, активлар, таҳдидлар, заифликлар, таъсир кўрсатишлар, хавфларни баҳолашда, шунингдек, катта ўзгаришларда. Хавфларни аниқлашда таққослаш ва қайта такрорлаш мумкин бўлган натижаларни ишлаб чиқиш учун бир методикадан фойдаланиш керак.

Ахборот хавфсизлигининг хавфларини аниқлаш самарали бўлиши учун унинг аниқ белгиланган қўлланиш соҳаси ва зарур бўлганда бошқа соҳалардаги хавфларни аниқлаш билан ўзаро боғлиқлик бўлиши керак.

Хавфларни аниқлаш қулай, амалга оширилиши мумкин ва фойдали бўлган ташкилот, ташкилотнинг қисмлари, алоҳида ахборот тизимлари, аниқ тизим компонентлари ёки сервислари хавфларни аниқлашни қўллаш соҳаси бўлиши мумкин. Хавфларни аниқлаш методологияларининг мисоллари ISO/IEC TR 13335-3 (АТ хавфсизлигини бошқариш бўйича тавсиялар: АТ хавфсизлигини бошқариш методикалари)да кўриб чиқилади.

4.2 Хавфсизлик хавфларига ишлов бериш

Хавфларга ишлов бериш натижаларини кўриб чиқишдан олдин ташкилот хавфларни қабул қилиш мезонларини аниқлаш бўйича қарор қабул қилиши керак. Агар хавф жуда кичик ва унга ишлов бериш баҳоси ташкилот учун фойдасиз бўлса, хавфлар қабул қилиниши мумкин. Ушбу қарорларни ёзиб қўйиш керак.

Ҳар бир аниқланган хавф учун улар аниқланганидан сўнг хавфларга ишлов бериш бўйича қарор қабул қилиниши керак. Хавфларга ишлов беришнинг қуйидаги вариантлари бўлиши мумкин:

a) хавфларни камайтириш учун қабул қилиниши мумкин бўлган бошқариш воситаларининг қўлланиши;

b) хавфларни ташкилот сиёсатига ва хавфларни қабул қилиш мезонларига аниқ тўғри келишини таъминлашда тушуниб етиш ва объектив қабул қилиш;

c) ушбу хавфларни келтириб чиқариши мумкин бўлган ҳаракатларни ман этиш йўли билан хавфлардан қочиш;

d) ўзаро боғлиқ бўлган хавфларни бошқа томонларга, масалан суғуртачилар ва таъминотчилар томонига юклаш.

Қабул қилиниши мумкин бўлган бошқариш воситаларини қўллаш йўли билан ишлов беришга қарор қилинган хавфлар учун ушбу бошқариш воситаларини хавфларни аниқлашда қўйилган талабларга мувофиқ танлаш ва жорий этиш керак. Бошқариш воситалари хавфлар қуйидагиларни қабул қилган ҳолда қабул қилса бўладиган даражагача пасайтирилганлигини кафолатлаши керак:

a) миллий ва халқаро қонун ҳужжатлари ва нормаларнинг талаблари ва чеклашлари;

b) ташкилот мақсадлари;

c) ишга оид талаблар ва чеклашлар;

d) жорий этиш нархи ва ташкилот талаблари ва чеклашларига пропорционал қоладиган пасайтириладиган хавфларга тегишли ишлар;

e) бошқариш воситаларини жорий этиш ва уларнинг ишига оид инвестицияларни, хавфсизликнинг бузилишидан етказилиши мумкин бўлган зарарни балансировка қилиш эҳтиёжи.

Бошқариш воситалари ушбу стандартдан, бошқариш воситаларининг бошқа тўпламларидан танланиши мумкин ёхуд ташкилотнинг муайян эҳтиёжларини қондириш учун янги бошқариш воситалари ишлаб чиқилиши мумкин. Шуни тушуниш керакки, баъзи бошқариш воситаларини муайян ахборот тизимига ёки атрофга қўлланиши мумкин бўлмаслиги, шунингдек ташкилот учун қулай бўлмаслиги мумкин. Масалан, 10.1.3-бандда фирибгарлик ва хатоларни олдини олиш учун мажбуриятлар қандай тақсимланиши мумкинлиги таърифланган. Катта бўлмаган ташкилотларда барча мажбуриятларни тақсимлаш учун имконият йўқ, шунинг учун бошқаришнинг мақсадларига эришиш учун бошқа усуллардан фойдаланиш мумкин. Бошқа мисол, 10.10-бандда тизимлардан фойдаланишни қандай кузатиш мумкинлиги ва далилларни қандай йиғиш мумкинлиги таърифланган. Таърифланган бошқариш воситалари, масалан, воқеаларни рўйхатга олиш, тегишли қонун ҳужжатларига, масалан, мижозлар ва ишчи ходимларнинг шахсий маълумотларини муҳофаза қилиш тўғрисидаги ҳужжатларга зид бўлиши мумкин.

Ахборот хавфсизлигини бошқариш воситаларини тизимларда ва лойиҳа талаблари спецификацияларида ишлаб чиқиш босқичида кўриб чиқиш мумкин. Акс ҳолда қўшимча сарф-харажатларга йўл қўйилиши ва самарасиз қарорлар жорий этилиши, шунингдек, зарур хавфсизликка эришилмаганлиги аниқланиши мумкин.

Шуни эсда тутиш керакки, бошқариш воситаларининг ҳеч қандай тўплами тўлиқ хавфсизликка эришишга имкон бермайди ва ташкилот мақсадларига эришишга ёрдам бериш учун хавфсизликни бошқариш воситаларини кузатиш, баҳолаш ва ишлаб чиқариш унумдорлиги ва самарадорлигини ошириш учун қўшимча равишда бошқарувчи хатти-ҳаракатлар жорий этилиши керак.

5 Хавфсизлик сиёсати

5.1 Ахборот хавфсизлигининг сиёсати

Мақсад: қонун ҳужжатлари, бизнес ва раҳбарий ҳужжатлар талабларига мувофиқ ахборот хавфсизлигини бошқариш ва сақлаб туриш масалаларининг ҳал қилинишини таъминлаш.

Раҳбарият сиёсатнинг аниқ йўналишини бизнес мақсадларига мувофиқ белгилаши, ахборот хавфсизлигини сақлаб туриши, бутун ташкилот бўйича ахборот хавфсизлиги сиёсатини ишлаб чиқиш ва амалга ошириш йўли билан унга тааллуқли мажбуриятларга риоя қилиши керак.

5.1.1 Ахборот хавфсизлиги сиёсатини ҳужжатли расмийлаштириш

Бошқариш воситаси

Ахборот хавфсизлигининг сиёсати тасдиқланган, нашр этилган ва ташкилотнинг барча ходимларига, зарур бўлганда, бегона ташкилотларга маълумот учун етказилган бўлиши керак.

Жорий этиш бўйича қўлланма

Ахборот хавфсизлигининг сиёсати раҳбариятнинг жавобгарлигини белгилаши, шунингдек ташкилотнинг ахборот хавфсизлигини бошқаришга ёндошишини баён этиши керак. У қуйидагиларга тааллуқли қоидаларни ўз ичига олиши керак:

a) ахборот хавфсизлиги, унинг асосий мақсадлари ва қўлланиш соҳасини аниқлаш, шунингдек, хавфсизлик маъносини ахборотдан биргаликда фойдаланиш имкониятини таъминлайдиган қурол сифатида очиб бериш (Кириш);

b) бошқариш мақсадлари, бизнес стратегияси ва мақсадларига мувофиқ ахборот хавфсизлигини қўллаб-қувватлаш бўйича масалалар ва принциплар;

c) бошқариш мақсадларини қўйиш структураси асосини ва бошқариш воситаларини аниқлашни, жумладан хавфларни аниқлаш ва хавфларни баҳолаш структураси;

d) ташкилот учун энг аҳамиятли хавфсизлик сиёсати, принциплари, қоида ва талабларини қисқа баён этиш, жумладан:

1) қонун ҳужжатларининг талаблари ва шартнома мажбуриятларига мувофиқлиги;

2) хавфсизлик соҳасида ўқитиш, тренинглар ва хабардорлигини ошириш бўйича талаблар;

3) ташкилотнинг узлуксиз ишини таъминлаш сиёсати;

4) ахборот хавфсизлиги сиёсатининг бузилиш оқибатлари;

e) ахборот хавфсизлигини бошқариш доирасида ходимларнинг умумий ва муайян мажбуриятларини, жумладан ахборот хавфсизлигининг бузилиш инцидентлари тўғрисида ахборот беришни белгилаш;

f) ахборот хавфсизлиги сиёсатини тўлдирувчи ҳужжатларга ҳаволалар, масалан муайян ахборот тизимлари учун аниқроқ сиёсат ва хавфсизлик процедуралари, шунингдек, фойдаланувчилар риоя қилиши керак бўлган хавфсизлик қоидалари.

Ахборот хавфсизлигининг ушбу сиёсатини ташкилотнинг барча фойдаланувчиларига маълумот учун, фойдаланса бўладиган ва тушунарли қилиб етказиш керак.

Бошқалар

Ахборот хавфсизлигининг сиёсати ташкилот сиёсатининг бир қисми бўлиши мумкин. Агар ахборот хавфсизлигининг сиёсати ташкилот ташқарисига тарқалса, конфиденциал ахборотни ошкор этмаслик учун эҳтиёткорликка риоя қилиш керак. Батафсил ахборот ISO/IEC 13335-1:2004 да мавжуд.

5.1.2 Ахборот хавфсизлигининг сиёсатини қайта кўриб чиқиш

Бошқариш воситаси

Ахборот хавфсизлиги сиёсатини белгиланган процедурага мувофиқ ёки катта аҳамиятга эга ташкилий ёки технологик инфратузилмавий ўзгаришлар бўлганда унинг адекватлиги, етарлилиги ва самарадорлилигини таъминлаш учун даврий равишда қайта кўриб чиқиш керак.

Жорий этиш бўйича қўлланма

Ташкилотда ахборот хавфсизлиги сиёсатини ишлаб чиқиш, қайта кўриб чиқиш ва баҳолаш учун жавобгар мансабдор шахс тайинланган бўлиши зарур. Қайта кўриб чиқиш учун ташкилий ёки технологик инфратузилмадаги, бизнес ҳолатлар ёки юридик шароитлардаги ўзгаришларга жавобан ахборот хавфсизлиги сиёсатини ва ахборот хавфсизлигини бошқаришга ёндашишни яхшилаш имкониятларини аниқлаш киритилиши керак.

Ахборот хавфсизлиги сиёсатини қайта кўриб чиқишни амалга оширишда раҳбарият текширувларининг натижаларини эътиборга олиш керак. Белгиланган жадвалга мувофиқ раҳбарият томонидан ўтказиладиган текширувларни ўтказиш тартиби белгиланган бўлиши керак.

Раҳбарият томонидан текширувлар ўтказилиши учун қуйидагилар объектив сабаблар бўлиб ҳисобланади:

a) манфаатдор томонларнинг мурожаатлари;

b) мустақил текширувлар натижалари (6.1.18);

c) огоҳлантирувчи ва тузатиш киритувчи хатти-ҳаракатларнинг ҳолати;

d) раҳбарият томонидан аввал ўтказилган текширувлар натижалари;

e) жараёнларнинг самаралилиги ва уларнинг ахборот хавфсизлиги сиёсатига мувофиқлиги;

f) ташкилот ахборот хавфсизлигини бошқаришга ёндашишга, жумладан ташкилий ёки технологик инфратузилмалардаги ўзгаришларга, бизнес ҳолатларига, активлардан фойдалана олиш мумкинлигига, шунингдек шартномавий, норматив ва юридик шароитларга таъсир этиши мумкин бўлган ўзгаришлар;

g) таҳдидлар ва заифликлар билан боғлиқ тенденциялар;

h) ахборот хавфсизлиги инцидентлари тўғрисида ҳисобот бериш (13.1);

i) тегишли давлат органларининг тавсиялари (6.1.6)

Текширув ўтказиш натижаларига кўра раҳбарият томонидан яхшилаш билан боғлиқ қарорлар қабул қилинади:

a) ташкилотнинг ахборот хавфсизлиги ва унинг жараёнларини бошқаришга ёндашиши;

b) бошқариш мақсадлари ва бошқариш воситалари;

c) активларни ва/ёки мажбуриятларни тақсимлаш;

Раҳбарият томонидан ўтказилган текширувлар натижаси тўғрисида ҳисобот тузилади.

Ахборот хавфсизлигининг қайта кўриб чиқилган сиёсати раҳбарият томонидан тасдиқланиши керак.

6 Ахборот хавфсизлигини таъминлашни ташкил қилиш

6.1 Ички ташкил қилиш

Мақсад: ташкилотда ахборот хавфсизлигини бошқариш.

Бошқариш структурасини шундай яратиш керакки, у ташкилотда ахборот хавфсизлигини жорий этиш назоратини инициация қилиш ва амалга оширишга ёрдам берсин.

Сиёсатни тасдиқлаш, жавобгар шахсларни тайинлаш, шунингдек, ташкилотда ахборот хавфсизлиги контекстида тадбирларни жорий этиш мувофиқлигини амалга ошириш учун юқори раҳбарият иштирокида тегишли бошқарувчи кенгашлар яратилиши керак.

Зарур бўлганда ташкилот ичида ахборот хавфсизлиги масалалари бўйича манфаатдор ходим мурожаат этиши мумкин бўлган мутахассис кўзда тутилиши керак. Соҳа тенденциялари, уни баҳолаш усуллари ва методларидан хабардор бўлиш, шунингдек, ахборот хавфсизлигининг бузилишига адекват муносабат билдириш мақсадида хавфсизлик бўйича ташқи мутахассислар билан алоқаларни яхшилаш керак. Ахборот хавфсизлигига кўп профиллик ёндашишни қўллаб-қувватлаш керак, масалан, менежерлар, фойдаланувчилар, маъмурлар, иловаларни ишлаб чиқувчилар, аудитлар ва хавфсизлик ходимлари, шунингдек, суғурталаш ва хавфларни бошқариш соҳасидаги мутахассислар ўртасида ҳамкорликни йўлга қўйиш йўли билан.

6.1.1 Раҳбарият томонидан ахборот хавфсизлигига тааллуқли мажбуриятларни бажариш

Бошқариш воситаси

Раҳбарият аниқ кўрсатмалар бериш, бажаришда намуна бўлиш, аниқ топшириқлар бериш, шунингдек, ахборот хавфсизлигини таъминлаш бўйича топшириқларни тасдиқлаш билан ташкилотда хавфсизликни фаол сақлаб туриши керак.

Жорий этиш бўйича қўлланма

Раҳбарият қуйидагиларни бажариши керак:

a) хавфсизлик мақсадлари белгиланганлиги, ташкилот талабларига мувофиқ ва тегишли жараёнларга киритилганлигига ишонч ҳосил қилиш;

b) ахборот хавфсизлигининг сиёсатини ифодалаш, қайта кўриб чиқиш ва тасдиқлаш;

c) ахборот хавфсизлигининг сиёсатини жорий этишнинг самаралилигини назорат қилиш;

d) хавфсизликни оширишга йўналтирилган ташаббускорликка сезиларли маъмурий қўллаб-қувватлашни ва аниқ раҳбарликни таъминлаш;

e) ахборот хавфсизлигини таъминлаш учун зарур активларнинг ажратилишини таъминлаш;

f) ташкилот ичида ахборот хавфсизлиги учун жавобгарларни тайинлашни ва уларнинг мажбуриятларини тасдиқлаш;

g) ходимларнинг ахборот хавфсизлиги бўйича хабардорлигини таъминлаш режалари ва дастурларини инициация қилиш;

h) ахборот хавфсизлигини бошқариш воситаларини ташкилот ичида жорий этиш мувофиқлаштирилганлигига ишонч ҳосил қилиш (6.1.2).

Раҳбарият ахборот хавфсизлиги бўйича ташкилотда ишлайдиган ва ташқаридан таклиф этилган мутахассисларнинг маслаҳатларига заруратни аниқлаши, шунингдек, ушбу маслаҳат натижаларини ташкилот миқёсида кўриб чиқиши ва мувофиқлаштириши керак.

Ташкилотнинг катта-кичиклигига қараб юқорида санаб ўтилган мажбуриятлар тегишли бошқарув кенгашига, бошқарувнинг коллегиал органига, ёхуд директорлар кенгаши каби мавжуд раҳбарлик инстанциясига юкланиши мумкин.

Бошқалар

Аниқроқ маълумот ISO/IEC 13335:2004 стандартида келтирилган.

6.1.2 Ахборот хавфсизлиги масалаларини мувофиқлаштириш

Бошқариш воситаси

Ташкилот турли манфаатдор бўлинмаларининг раҳбарлари ахборот хавфсизлигини бошқариш бўйича тадбирларни жорий қилиш масалаларини мувофиқлаштиришлари керак.

Жорий этиш бўйича қўлланма

Одатда, ахборот хавфсизлиги масалаларини мувофиқлаштириш раҳбарият, фойдаланувчилар, маъмурлар, иловаларни ишлаб чиқувчилар, аудиторлар ва хавфсизлик ходимлари, шунингдек, суғурта қилиш, юриспруденция, кадрлар иши, АТ ёки хавфларни бошқариш каби соҳаларда кўникмаларга эга бўлган мутахассисларнинг биргаликдаги ҳаракати ва ҳамкорлигини ўз ичига олиши керак. Ушбу фаолият жараёнида:

a) хавфсизлик чоралари ахборот хавфсизлиги сиёсатига мувофиқ бажарилаётганлигига ишонч ҳосил қилиш;

b) номувофиқлик ҳолатларининг ишлов бериш усулларини аниқлаш;

c) ахборот хавфсизлиги методологияси ва жараёнларини, масалан, хавфларни аниқлашни, ахборотни таснифлашни тасдиқлаш;

d) таҳдидларнинг сезиларли ўзгаришларини ҳамда ахборот ва унга ишлов бериш воситалари таҳдидларга учраган моментларни аниқлаш;

e) ахборот хавфсизлигини бошқариш воситаларининг адекватлилигини ва жорий этилишини мувофиқлаштиришни баҳолаш;

f) ахборот хавфсизлиги соҳасида ўқитиш, тренинглар ва хабардорликни ташкилот миқёсида самарали қўллаб-қувватлаш;

g) хавфсизлик инцидентларини аниқлаш ва уларга ишлов бериш натижасида олинган ахборотни таҳлил қилиш, шунингдек, ахборот хавфсизлигининг белгиланган инцидентларига жавобан қабул қилиниши мумкин бўлган чораларни тавсия этиш.

Агар ташкилотда алоҳида бошқарувчи кенгаш тайинланмаган бўлса, масалан ташкилотнинг миқёсига тўғри келмаганлиги учун, унда юқорида таърифланган хатти-ҳаракатларни бошқа раҳбарлик қилувчи орган ёки алоҳида раҳбар амалга ошириши керак.

6.1.3 Ахборот хавфсизлигини таъминлаш бўйича мажбуриятларни тақсимлаш

Бошқариш воситаси

Ахборот хавфсизлигини таъминлаш бўйича барча мажбуриятлар аниқ белгиланган бўлиши керак.

Жорий этиш бўйича қўлланма

Ахборот хавфсизлиги бўйича мажбуриятларнинг тақсимлани-шини ахборот хавфсизлиги (5.1) сиёсатига мувофиқ бажариш керак. Шахсий маълумотларни муҳофаза қилиш ва хавфсизликнинг муайян жараёнларини бажариш бўйича мажбуриятларни аниқ белгилаш керак.

Зарурат бўлганда мажбуриятларни муайян объектлар ва ахборотга ишлов бериш воситалари учун янада аниқроқ тавсиялар билан тўлдириш керак. Активларни муҳофаза қилиш ва хавфсизликнинг узлуксиз ишни режалаштириш каби аниқ жараёнларини бажариш бўйича локал мажбуриятларни аниқ белгилаш керак.

Ахборот хавфсизлигини таъминлаш бўйича масалаларни бажариш учун жавобгар ходим ўз мажбуриятларини кимгадир юклаши мумкин. Шундай бўлса ҳам, у жавобгар бўлиб қолади ва ҳар бир юкланган топшириқнинг тўғри бажарилишини таъминлаши керак.

Ходим жавобгар бўлган соҳаларни аниқ ифодалаш керак; хусусан қуйидаги тадбирларни амалга ошириш зарур:

a) хавфсизликнинг ҳар бир алоҳида тизим билан боғлиқ активлари ва жараёнларини аниқлаш ва аниқ белгилаш керак;

b) хавфсизликнинг ҳар бир актив ва жараёни учун жавобгарни тайинлаш, шунингдек, ушбу мажбуриятларни ҳужжатлаштириш керак (7.1.2);

c) ваколатлар даражасини аниқ белгилаш ва ҳужжатлаштириш.

Бошқалар

Кўпгина ташкилотларда ташкилот раҳбарлари аъзоларидан ахборот хавфсизлиги билан боғлиқ барча масалаларга жавобгар тайинланади.

Бироқ активларни қидириш ва бошқриш воситаларини жорий этиш учун жавобгарлик кўпинча алоҳида раҳбарлар зиммасида қолади. Ҳар бир активга унинг кундалик муҳофазаси учун жавобгар бўлиб қоладиган эгасини тайинлаш кенг тарқалган тажрибага айланмоқда.

6.1.4 Ахборотга ишлов бериш воситаларидан фойдаланиш учун рухсат олиш жараёни

Бошқариш воситаси

Ахборотга ишлов беришнинг янги воситаларидан фойдаланиш учун рухсат олиш процедураларини аниқлаш ва жорий этиш зарур.

Жорий этиш бўйича қўлланма

Рухсат олиш процедураларини жорий этиш учун қуйидаги тадбирлар бажарилиши керак:

a) янги воситалар ва уларнинг вазифаси фойдаланувчиларнинг раҳбарлари томонидан тасдиқланган ва локал ахборот тизимлари ишлашининг хавфсиз муҳитини кузатиш учун жавобгар маъмур томонидан маъқулланган бўлиши керак. Ушбу чоралар хавфсизликнинг тегишли сиёсатлари ва талабларини бажаришни кафолатлашга имкон беради;

b) аппарат воситалари ва дастурий таъминотни тизимнинг бошқа компонентлари билан мослашувчанлигига текшириш керак;

d) иш жойида хизматга оид ахборотга ишлов бериш учун ахборотнинг шахсий ишлов бериш воситаларидан, масалан, ноутбуклар, уй компьютерлари ва бошқалардан фойдаланиш янги заифликларнинг сабаби бўлиши мумкин ва бинобарин таъсири баҳоланган ва тасдиқланган бўлиши керак.

6.1.5 Конфиденциалликни сақлаш тўғрисида контрактлар

Бошқариш воситаси

Ташкилотда амалда бўлган ахборот хавфсизлиги сиёсатлари асосида ишлаб чиқилган конфиденциалликни сақлаш ва ошкор этмаслик тўғрисидаги контрактларга қўйиладиган талабларни белгилаш ва мунтазам қайта кўриб туриш керак.

Жорий этиш бўйича қўлланма

Конфиденциалликни сақлаш ва ошкор этмаслик тўғрисида контрактлар норматив-ҳуқуқий ҳужжатларда белгиланган конфиденциал ахборотни муҳофаза қилиш бўйича талабларга жавоб бериши керак. Конфиденциалликни сақлаш ва ошкор этмаслик тўғрисида контрактларга қўйилган талабларни белгилашда қуйидаги жиҳатларга амал қилиш керак:

a) муҳофаза қилинаётган ахборотнинг таснифи (масалан конфиденциал ахборот);

b) контрактнинг кутилаётган амал қилиш муддати, жумладан конфиденциалликка риоя қилиш муддатсиз бўлган ҳолларни ҳам ҳисоблаганда;

c) контрактнинг амал қилиш муддати тўхтатилган ҳолларда зарур чоралар;

d) ахборотни («билишнинг зарурлик принципи», «фақат билиш зарур бўлган нарсани билиш» каби) рухсатсиз ошкор этилишига йўл қўймаслик учун контрактни имзоловчи шахслар жавобгарлиги ва хатти-ҳаракатлари;

e) конфиденциал ахборотни муҳофаза қилиш билан тижорат сири ва интеллектуал эгалик ўртасидаги боғлиқлик;

f) конфиденциал ахборотдан фойдаланишга рухсат беришда контрактни имзолаётган шахснинг мажбуриятлари ва ҳуқуқлари;

g) конфиденциал ахборотдан фойдаланиш аудити ва мониторингини ўтказиш;

h) рухсатсиз ошкор этиш ва конфиденциалликни бузиш ҳолатлари тўғрисида хабар ва ҳисобот бериш тартиби;

i) контрактнинг муддати тугаган ҳолларда ахборот йўқ қилиниши ёки қайтарилиши керак бўлган муддатларни белгилаш;

j) контракт бузилганда кўриладиган чоралар.

Ташкилотдаги хавфсизлик сиёсати талабларига асосан конфиденциалликка риоя қилиш ва ошкор этмаслик тўғрисида бошқа контрактларга зарурат туғилиши мумкин.

Конфиденциалликка риоя қилиш ва ахборотни ошкор этмаслик тўғрисидаги контрактлар амалдаги қонун ҳужжатлари ва юридик талабларга мос келиши керак (15.1.1).

Конфиденциалликка риоя қилиш ва ахборотни ошкор этмаслик тўғрисидаги контрактларга қўйилган талабларни ушбу талабларга таъсир қиладиган ўзгаришлар бўлганда вақти-вақти билан қайта кўриб чиқиш керак.

Бошқалар

Конфиденциалликка риоя қилиш ва ошкор этмаслик тўғрисидаги контрактлар ташкилот ахборот активларини муҳофаза қилиш учун мўлжалланган. Ушбу контрактларни имзоловчи шахслар рухсатсиз фойдаланганликлари ва конфиденциал ахборотни ошкор этганликлари учун жавобгардирлар.

Турли ҳолатларда ташкилотга конфиденциалликка риоя қилиш ва ошкор этмаслик тўғрисидаги контрактларнинг турли шакллари керак бўлиб қолиши мумкин.

6.1.6 Давлат органлари билан алоқалар

Бошқариш воситаси

Тегишли давлат органлари билан керак бўлган алоқалар ўрнатилиши керак.

Жорий этиш бўйича қўлланма

Ташкилотда ким ва қачон давлат органлари (масалан, ички ишлар органлари, ёнғин мудофааси органлари, назорат органлари) билан боғланиши кераклигини белгиловчи, шунингдек, агар қонун ҳужжатларининг бузилишига гумон бўлса, ахборот хавфсизлигининг аниқланган инцидентлари тўғрисида хабар бериш вақтини регламентга солувчи тартиб белгиланган бўлиши керак.

Турли хил ҳужумларга, жумладан Интернет тармоғидан бўладиган ҳужумларга ҳам қарши ҳаракат қилиш бўйича тегишли чораларни қўллаш учун бегона ташкилотлар, (масалан, Интернет тармоғи провайдери ёки

телекоммуникациялар оператори)нинг ёрдами керак бўлиб қолиши мумкин.

Бошқалар

Ушбу алоқаларни ўрнатиш ахборот хавфсизлиги инцидентларини бошқариш бўйича талабларга (13.2) ва узлуксиз ишни таъминлаш ҳамда фавқулодда вазиятларни режалаштириш (14) жараёнларига мувофиқ амалга оширилиши керак. Қонун чиқарувчи органлар билан алоқалар ташкилотлар томонидан риоя қилиниши керак бўлган норматив ҳужжатларга ўзгартиришлар тайёрлашда бевосита иштирок этиш учун фойдалидир. Алоқалар ўрнатилиши керак бўлган бошқа органларга коммунал хизматлари, тез ёрдам хизматлари, ёнғин мудофааси хизматларини (бизнес узлуксизлигига тааллуқли), телекоммуникациялар операторларини (уловчи линияларнинг маршрутлаштирилиши ва қулайлилигига нисбатан) сув етказиб берувчилар (ускуна учун совитиш воситаларига тегишли)ни киритиш мумкин.

6.1.7 Тематик гуруҳлар билан алоқалар

Бошқариш воситаси

Тематик гуруҳлар, хавфсизлик бўйича мутахасссислар форуми ёки профессионал ассоциациялар билан тегишли алоқаларни ўрнатиш керак.

Жорий этиш бўйича қўлланма

Тематик гуруҳлар ёки форумларга аъзоликка қуйидагиларни амалга ошириш усули сифатида қараш керак:

a) ахборот хавфсизлигини таъминлаш соҳасидаги замонавий, илғор амалий қарорлар тўғрисида хабардорлигини ошириш;

b) ахборот хавфсизлиги муҳитини тушуниш замонавий ва тўлиқ ҳисобланишини тасдиқлаш;

c) ҳужумлар ва заифликларга тегишли хавфлар тўғрисида барвақт огоҳлантиришлар, тавсиялар ва ямоқлар олиш;

d) ахборот хавфсизлиги бўйича мутахассислардан маслаҳатлар олиш;

e) янги технологиялар, маҳсулот, таҳдидлар ва заифликлар тўғрисидаги ахборотдан биргаликда фойдаланиш ва айирбошлаш;

f) ахборот хавфсизлиги инцидентлари юзага келганида алоқаларни йўлга қўйиш (13.2.1).

Бошқалар

Ҳамкорликни яхшилаш ва ахборот хавфсизлиги билан боғлиқ масалаларни мувофиқлаштириш учун ахборотдан биргаликда фойдаланиш тўғрисида контрактлар тасдиқланиши мумкин. Ушбу контрактлар конфиденциал ахборотни муҳофаза қилишга қўйилган талабларни белгилаши керак.

6.1.8 Ахборот хавфсизлигининг мустақил текшируви (аудит)

Бошқариш воситаси

Ташкилотда ахборот хавфсизлигини бошқариш бўйича тадбирларни амалга ошириш (яъни бошқариш воситалари, сиёсат, ахборот хавфсизлиги жараёнлари ва процедуралари) ишлаб чиқилган режа асосида ёхуд хавфсизлик бўйича тадбирларни амалга оширишда катта ўзгаришлар юз берганида мустақил текширилиши (аудит) керак

Жорий этиш бўйича қўлланма

Мустақил текширув раҳбарият томонидан инициация қилинади. У ташкилотда ишлаб чиқилган тадбирлар керак тарзда сиёсатни акс эттиришига, бажарса бўладиган ва самарали ҳисобланишига ишончни таъминлаш мақсадида ўтказилади.

Ушбу текширув мумкин бўлган яхшиланишларнинг баҳоланишини, шунингдек, бошқариш сиёсати ва мақсадларини ҳисобга олган ҳолда хавфсизликка ёндашишнинг ўзгаришларига эҳтиёжни аниқлаши керак.

Бундай текширув ички аудит, мустақил менежер ёки ана шундай текширувларда ихтисослашган бегона ташкилот томонидан бажарилиши мумкин, бунда текширувга жалб этиладиган мутахассислар тегишли кўникма ва тажрибага эга бўлишлари керак.

Мустақил текширув натижаларини ёзиш ва ушбу текширувни инициация қилган раҳбарга ҳисобот кўринишида юбориш керак. Берилган ҳужжатлар таҳлил қилиниши керак.

Агар текширув томонидан ахборот хавфсизлигини бошқариш бўйича тадбирларни амалга ошириш ахборот хавфсизлиги талаблари ва нормаларига мос келмаслиги (5.1.1) аниқланса, раҳбарият тузатишлар киритиш тўғрисидаги масалани кўриб чиқиши керак.

Бошқалар

Раҳбарият томонидан мунтазам текширлиб турадиган соҳалар (15.2.1) ҳам, мустақил текширув объекти бўлиши мумкин. Текширув технологиялари раҳбар билан суҳбатни, ёзувларни текшириш ва хавфсизлик сиёсати ҳужжатларини таҳлил қилишни ўз ичига олади. Мустақил текширувни ўтказиш учун фойдали қўлланмалар, жумладан текширув дастурини тасдиқлаш ва амалга ошириш ISO 19011:2002 «Сифат менежменти ва/ёки атроф-муҳит тизимларининг аудити бўйича кўрсатмалар» стандартида келтирилган. 15.3-бандда амалдаги ахборот тизимларини мустақил текшириш учун мақбул бошқариш воситалари, шунингдек, тизим аудитининг ишлатиладиган асбоблари санаб ўтилган.

6.2 Бегона ташкилотлар

Мақсад: ахборот хавфсизлиги ва унга ишлов бериш воситаларини сақлаш, шунингдек, бегона ташкилотлар фойдаланиши мумкин бўлган ташкилот ахборот активлари хавфсизлигини таъминлаш.

Ташкилотга қарашли ахборот ва унга ишлов бериш воситаларининг хавфсизлиги бегона ташкилотлар маҳсулотидан ва улар томонидан тақдим этилган хизматлардан фойдаланганлиги учун пасайиши керак эмас.

Бегона ташкилотларнинг ташкилотга қарашли ахборотга ишлов бериш воситаларидан, ахборотга ишлов бериш ва уни узатиш жараёнларидан фойдаланишини бошқариш керак.

Бегона ташкилотлар ташкилотнинг ахборот активлари ва ахборотга ишлов бериш воситаларидан ишлаб чиқариш сабабаларига кўра фойдаланиши зарур бўлган жойларда, шунингдек, бегона ташкилотлардан товар олиш ва уларнинг хизматларидан фойдаланиш ҳолларида ахборот ва бошқариш воситаларига қуйилган талабларнинг хавфсизлиги учун мумкин бўлган оқибатларни аниқлаш учун хавфларни таҳлил қилиш керак.

Бундай тадбирларни бегона ташкилот билан тузилган контрактда келишиш ва белгилаш керак.

6.2.1 Бегона ташкилотлар билан боғлиқ хавфларни аниқлаш

Бошқариш воситаси

Томонлар иштирок этадиган бизнес-жараёнлар томонидан ташкилотга тегишли ахборот ва унга ишлов бериш воситаларига тегишли хавфларни аниқлаш керак. Фойдаланишга рухсат беришдан аввал мақбул бошқариш воситаларини жорий этиш керак.

Жорий этиш бўйича қўлланма

Агар бегона ташкилотларнинг ахборотга ишлов бериш воситаларидан ва/ёки ташкилот ахборот активларидан фойдаланишлари учун рухсат бериш зарурати бўлса, у ҳолда муайян бошқариш воситаларига талаблар қўйиш учун хавфларни белгилаш керак (4). Бегона ташкилотларнинг фойдалана олишига тегишли хавфларни аниқлашда қуйидагиларни эътиборга олиш керак:

a) бегона ташкилотлар фойдаланиши керак бўлган ахборотга ишлов бериш воситалари;

b) бегона ташкилотнинг ахборот ва унга ишлов бериш воситаларидан фойдаланиш тури, масалан:

1) офис хоналари, компьютер хоналари, сервер хоналаридан - жисмоний фойдаланиш;

2) ташкилотнинг маълумотлар базалари ва ахборот тизимларидан - мантиқий фойдаланиш;

3) ташкилот тармоқлари ва бегона ташкилот ўртасида тармоқли уланиш - доимий уланиш ёки узоқлаштирилган фойдаланиш;

4) фойдаланиш эксплуатация қилиш жойида тақдим этиладими ёки ундан ташқаридами;

c) амалдаги ахборотнинг муҳимлиги ва конфиденциаллиги, шунингдек, бизнес-операциялар учун унинг сезгирлиги;

d) ташкилотнинг ахборот активларини муҳофаза қилиш учун зарур бўлган ва бегона ташкилотларга фойдаланишни тақдим этиш учун мўлжалланмаган бошқариш воситалари;

e) ташкилот ахборотига ишлов беришда қатнашадиган бегона субпудратчининг ходими;

f) фойдаланишга рухсат олишга ваколат берилган ташкилот ёки ходимни идентификация қилиш усули, ваколатларни, шунингдек, эҳтиёжларни тасдиқлашнинг такрорланишини текшириш усули.

g) ахборотни сақлаш, унга ишлов бериш, уни узатиш, ундан биргаликда фойдаланиш ва алмашиш учун бегона ташкилотлар томонидан фойдаланиладиган турли усуллар ва бошқариш воситалари;

h) бегона субпудратчига ахборотдан зарур бўлган фойдаланишни инкор этишнинг таъсири, шунингдек, унинг томонидан ноаниқ ёки чалғитадиган ахборотни киритиш ва олиш;

i) ахборот хавфсизлиги инцидентлари ва потенциал зарарлар билан боғлиқ амалиёт ва процедуралар, ахборот хавфсизлиги инциденти ҳолатида бегона ташкилотнинг фойдаланишини давом эттириш муддатлари ва шартлари;

j) юридик ва норматив талаблар, шунингдек, эътиборга олиниши керак бўлган бегона ташкилотларга тегишли бошқа шартнома мажбуриятлари;

k) контрактларнинг ҳар қандай бошқа манфаатдор томонларнинг манфаатларига таъсири.

Мақбул бошқариш воситалари жорий этилмагунича бегона ташкилотга ташкилотнинг ахборот активларидан фойдаланиш учун рухсат берилмаслиги керак ва агар буни амалга ошириш мумкин бўлса, уланиш ёки фойдаланиш муддати ва шартларини, шунингдек, ишга оид келишувлар имзоланиши керак. Одатда, бегоналарнинг фойдаланиши ёки ахборот хавфсизлигини бошқариш бўйича тадбирлар билан боғлиқ хавфсизликнинг барча талабларини бегона ташкилот билан тузилган контрактда акс эттириш керак (6.2.2, 6.2.3).

Бегона ташкилот ўзининг мажбуриятларидан хабардорлигига, ахборотдан фойдаланиш, унга ишлов бериш, уни узатиш ва бошқаришга доир мажбуриятлар ва жавобгарликларни, шунингдек, ташкилотга мансуб ишлов бериш воситаларини қабул қилишига ишонч ҳосил қилиш керак.

Бошқалар

Ташкилот ахбороти бегона ташкилотлар хавфсизликни ноадекват бошқариб фойдаланганда хавфсизликни бошқариш даражаси етарли бўлмаганлиги учун хавфсизлигининг бузилиш хавфи пайдо бўлиши мумкин. Бегона ташкилотларнинг ахборотга ишлов бериш воситаларидан фойдаланишини идора қилиш бўйича бошқариш воситаларини ўрнатиш ва қўллаш керак. Масалан, агар ахборотнинг конфиденциаллигини таъминлашда алоҳида эҳтиёж мавжуд бўлса, уни ошкор қилмаслик тўғрисида контракт тузиш керак.

Ташкилотлар, агар аутсорсингнинг юқори даражаси қўлланса ёхуд бир неча бегона ташкилотлар ишлаётган бўлса, ташкилот коммуникацияларини бошқаришнинг ички жараёнлари билан боғлиқ хавф-ларга дучор бўлишлари мумкин.

Бошқариш воситалари (6.2.2, 6.2.3) турли бегона ташкилотлар билан тузиладиган контрактларни, жумладан қуйидагиларни баён қиладилар:

a) Интернет тармоғининг провайдерлари, телефон хизматлари, эксплуатацион хизматлар ва қўллаб-қувватлаш хизматлари каби хизматларнинг етказиб берувчилари;

b) бошқариладиган хавфсизлик хизматлари;

c) мижозлар;

d) воситалар ва/ёки операциялар аутсорсинги, масалан. АТ тизимлари, ахборот тўплаш сервислари, қўнғироқларга ишлов бериш марказининг;

e) менежмент ва бизнес бўйича маслаҳатчилар, шунингдек, аудиторлар;

f) аппарат воситалари ва дастурий таъминотни сақлаб турадиган ва кузатадиган ходимлар;

g) йиғиштириш, қўриқлашни амалга оширадиган, умумий овқатланиш ва бошқа хўжалик хизматларини таъминлайдиган ходимлар;

h) вақтинчалик ходимлар, студентлар ва меҳнат шартномалари бўйича ишлайдиган шахслар.

Ушбу контрактлар бегона ташкилотлар билан боғлиқ хавфларни камайтиришга ёрдам бериши мумкин.

6.2.2 Мижозлар билан бўладиган муносабатларда хавфсизлик чоралари

Бошқариш воситаси

Мижозларга ташкилот ахбороти ва активларидан фойдаланишга рухсат беришдан олдин хавфсизликнинг барча белгиланган талабларига эътибор қилиш керак.

Жорий этиш бўйича қўлланма

Мижозларга ташкилотнинг исталган активларидан фойдаланишга рухсат беришдан олдин (тақдим этилаётган фойдаланишнинг ҳаммаси ҳам қўлланиши мумкин бўлавермайдиган тури ва даражасига қараб) хавфсизликка тааллуқли бўлган қуйидаги шартларни ҳисобга олиш керак:

a) қуйидагиларни ўз ичига олган активларни муҳофаза қилиш:

1) ташкилот активларини, жумладан ахборот ва дастурий таъминотни, шунингдек, маълум заифликларни бошқариш бўйича процедуралар;

2) активларни компрометация қилиш фактини аниқлаш процедуралари, масалан, маълумотларни йўқотиш ёки модификация қилиш натижасида;

3) активларнинг бутлиги;

4) ахборотдан нусха кўчириш ва уни очишга қўйилган чеклашлар;

b) тақдим этилаётган товар ва хизматлар таърифи;

c) турли шартлар, талаблар ва мижозларнинг фойдаланишидан олинган фойда;

d) қуйидагиларни ўз ичига қамраган фойдаланишни бошқариш бўйича контрактлар:

1) фойдаланишнинг рухсат этилган методлари, шунингдек, фойдаланувчиларнинг ноёб идентификаторлари ва паролларини бошқариш ва улардан фойдаланиш;

2) фойдаланишга имтиёзлар ва ваколатлар тақдим этиш жараёни;

3) ҳар қандай фойдаланишни ман этиш принципи, равшанки рухсат берилмаганини;

4) фойдаланувчиларнинг фойдаланиш ҳуқуқларини қайтариб олиш ёки фойдаланишни блокировкалаш;

e) ҳисобот бериш, ахборот хавфсизлигининг бузилиш инцидентларидан хабардор бўлиш ва текшириш ҳамда хавфсизлик тизимининг заиф бўғимларини аниқлаш процедуралари;

f) фойдаланиш учун мўлжалланган ҳар бир сервисни таърифлаш;

g) сервиснинг режага оид даражаси ва сервиснинг йўл қўйиб бўлмайдиган даражалари;

h) мониторинг ҳуқуқи ва ташкилот активлари билан боғлиқ ҳар қандай фаолиятни бекор қилиш;

i) ташкилот ва мижознинг тегишли мажбуриятлари;

j) юридик масалалар ва қонун ҳужжатлари талабларига, масалан, агар контракт хориждаги мижозлар билан ҳамкорликни ўз ичига олса, турли миллий қонунчилик тизимларини эътиборга олган ҳолда маълумотларни муҳофаза қилиш тўғрисида қонунларга мувофиқлигини таъминлаш усулларига тегишли мажбуриятлар;

k) интеллектуал мулк эгалиги ҳуқуқлари ва муаллифлик ҳуқуқлари (15.1.2), шунингдек, ҳар қандай биргаликдаги ишни муҳофаза қилиш (6.1.5).

Бошқалар

Ташкилот активларидан фойдаланиш ҳуқуқига эга бўладиган мижозларга тегишли хавфсизлик талаблари тақдим этилаётган ахборот ва унга ишлов бериш воситаларини таснифлашга боғлиқ ҳолда катта фарқ қилиши мумкин. Ушбу хавфсизлик талаблари барча маълум хавфлар ва хавфсизлик талабларини ўз ичига оладиган, мижоз билан тузиладиган контрактда акс эттирилиши мумкин (6.2.1).

Бегона ташкилотлар билан тузиладиган контракт хавфсизликнинг бошқа талабларини ҳам ўз ичига олиши мумкин. Бегона ташкилотга фойдаланишни тақдим этиш учун тузилган контрактда бошқа қабул қилиниши мумкин бўлган томонларни жалб этишга рухсат бериш, шунингдек, уларнинг фойдаланиш ва қатнашиш шартлари кўрсатилиши зарур.

6.2.3 Бегона ташкилотлар билан тузиладиган контрактларда хавфсизлик чоралари

Бошқариш воситаси

Бегона ташкилотлар билан тузиладиган, ташкилотнинг ахборот активларидан, шунингдек, ахборотга ишлов бериш воситаларидан фойдаланиш, уларга ишлов бериш, уларни узатиш ёки бошқаришга, ахборотга ишлов бериш воситаларига маҳсулот ёки хизматларни қўшишга рухсат берадиган контрактларда хавфсизликнинг барча тегишли талаблари ёритилиши керак.

Жорий этиш бўйича қўлланма

Контрактда ташкилот ва бегона ташкилот ўртасида келишмовчиликлар бўлмаслиги керак. Ташкилот бегона ташкилотларнинг зарарларни қоплаши бўйича мажбуриятлари масалаларида эҳтиёт бўлиши керак.

Хавфсизликнинг белгиланган талабларини қондириш учун контрактга қуйидаги шартларни киритиш маслаласи кўриб чиқилиши керак:

a) ахборот хавфсизлигининг сиёсати;

b) активларнинг муҳофазасини таъминловчи бошқариш воситалари, жумладан:

1) ташкилот активларини, жумладан ахборот, дастурий ва аппарат таъминотини муҳофаза қилиш процедуралари;

2) жисмоний муҳофазанинг ҳар қандай зарур бошқариш воситалари ва механизмлари;

3) зарар келтирувчи дастурий таъминотдан муҳофаза қилиш учун ахборот хавфсизлигини бошқариш бўйича тадбирлар (10.4.1);

4) активларни компрометация қилиш фактини аниқлаш процедуралари, масалан дастурий ва аппарат таъминоти маълумотларини йўқотиш ёки модификация қилиш натижасида;

5) контракт амал қилиш муддати тугаши ёки контракт амал қилиш муддати давомида ахборот ва активларниинг қайтарилиши ва йўқ қилинишини таъминлаш бўйича тадбирлар;

6) ахборот ативларининг конфиденциаллиги, бутлиги, қулайлиги ва бошқа исталган тегишли хусусиятлари (2.5);

7) ахборотдан нусха кўчириш ва уни фош этишга чеклашлар, шунингдек, конфиденциаллик тўғрисида контрактлардан фойдаланиш (6.1.5);

c) фойдаланувчиларни ва маъмуриятни хавфсизлик методлари, процедуралари ва қоидаларига ўқитиш;

d) фойдаланувчиларнинг жавобгарлиги тўғрисида ва ахборот хавфсизлиги муаммолари тўғрисида хабардорлигини таъминлаш;

e) ходимларнинг (зарурат бўлганда) йўл қўйилиши мумкин бўлган кўчиш шартлари;

f) аппарат ва дастурий таъминотни ўрнатиш ва кузатишга тегишли мажбуриятлар;

g) ҳисобдорликнинг аниқ структураси ва ҳисоботларни тақдим этишнинг келишилган форматлари;

h) ўзгаришларни бошқаришнинг аниқ ва тўғри белгиланган жараёни;

i) қуйидагиларни ўз ичига олган фойдаланишни бошқариш сиёсати:

1) бегона ташкилотларнинг фойдаланишига рухсат бериш заруратининг турли шартлари, талаблари ва фойдалари;

2) фойдаланишнинг рухсат берилган методлари, шунингдек, фойдаланувчилар ва паролларнинг ноёб идентификаторларини бошқариш ва улардан фойдаланиш;

3) фойдаланишга имтиёзлар ва ваколатлар тақдим этиш жараёни;

4) тақдим этиладиган хизматлардан фойдаланиш ҳуқуқига эга бўлган шахслар рўйхатини юритиш бўйича талаб ва уларга тақдим этиладиган ҳуқуқлар ҳамда имтиёзларнинг таърифи;

5) ҳар қандай фойдаланишни ман этиш принципи, равшанки рухсат берилмаганини;

j) ахборот хавфсизлигининг бузилиш инцидентларининг ҳисобот, хабар бериш ва текшириш ҳамда хавфсизлик тизимининг заиф бўғимларини аниқлаш процедуралари;

k) тақдим этиладиган маҳсулот ёки хизматларнинг таърифи, шунингдек, хавфсизлик бўйича таснифланишига мувофиқ фойдаланиш рухсат этилган ахборот активининг таърифи (7.2.1);

1) зарур ва қабул қилиб бўлмайдиган хизмат кўрсатиш даражасини аниқлаш;

m) самарадорликнинг ўлчанадиган кўрсаткичларини аниқлаш, шунингдек, уларнинг мониторинги ва ҳисоботини тақдим этиш;

n) фойдаланувчилар хатти-ҳаракатининг мониторинги ва фойдаланишни блокировкалаш ҳуқуқи;

o) мажбуриятлар шартномаси бўйича кўзда тутилган аудит ўтказиш ёки учинчи томон томонидан ўтказилган аудит натижаларини олиш ҳуқуқи, шунингдек, аудиторни унинг уставида белгиланган ҳуқуқлари билан таништириш ҳуқуқи;

p) кутилмаган ҳолатларда юзага келган муаммолар тўғрисида хабар бериш жараёнини аниқлаш;

q) ташкилотнинг устуворлигига мувофиқ хизмат кўрсатишнинг узлуксизлик талаби, жумладан, қулайлик ва ишончлиликни таъминлаш чоралари;

r) томонларнинг контракт доирасида тегишли мажбуриятлари;

s) юридик масалаларга тегишли мажбуриятлар, масалан маълумотларни муҳофаза қилиш тўғрисидаги қонун ҳужжатлари, жумладан турли миллий қонун ҳужжатлари, айниқса, агар контракт турли мамлакатлар ўртасидаги ҳамкорликка тааллуқли бўлса (15.1);

t) интеллектуал мулк эгалиги ҳуқуқлари ва муаллифлик ҳуқуқлари (15.1.2), шунингдек, ҳар қандай биргаликдаги ишни ҳуқуқий муҳофаза қилиш (6.1.5).

u) бегона ташкилотларни субпудратчилар билан бирга жалб этиш, шунингдек, субпудратчилар томонидан амалга оширилиши керак бўлган хавфсизликни бошқариш воситаларидан фойдаланиш;

v) контрактни қайта тузиш/амал қилишини тўхтатиш шартлари;

1) агар истаган томон муносабатларни муддатидан аввал тўхтатишни истаса, фавқулодда вазиятларга муносабат билдириш режаси зарур бўлади;

2) агар ташкилотнинг хавфсизлик талаблари ўзгарса, контрактни қайта имзолаш;

3) активлар рўйхати, лицензиялар, контрактлар ёки уларга тааллуқли ҳуқуқлар бўйича кундалик ҳужжатлар.

Бошқалар

Турли ташкилотлар ва бегона ташкилотларнинг турли хиллари учун контрактлар сезиларли даражада фарқ қилиши мумкин, шунинг учун хавфсизликнинг барча аниқланган хавфлари ва талабларини контрактга киритишда эҳтиёткорликка риоя қилиш керак (6.2.1). Зарур бўлганда хавфсизликни бошқариш режасида талаб қилинган бошқариш воситалари ва процедуралар кенгайтирилиши мумкин.

Агар ахборот хавфсизлигини бошқариш бегона ташкилот томонидан таъминланса, унда контрактларда хавфларни аниқлашда белгиланган етарли бўлган хавфсизликни сақлаб туриш қай тарзда кафолатланиши, шунингдек, хавфларни аниқлашда ва ўзгартиришда хавфсизлик қай тарзда сақлаб турилишини ҳисобга олиш керак.

Аутсорсинг ва сервисни бегона ташкилотлар томонидан тақдим этишнинг бошқа шакллари ўртасидаги фарқларга жавобгарлик, ўтиш даврини режалаштириш ва ушбу давр давомида операцияларнинг потенциал бузилиши, фавқулодда вазиятларга муносабат билдиришни режалаштириш бўйича тадбирлар, шунингдек, инцидентлар билан боғлиқ ахборотни йиғиш ва бошқариш масалалари киради. Бинобарин, ташкилот режага эга бўлиши ва бегона ташкилот томонидан тадбирлар ўтказилишига ўтишни бошқариши, шунингдек, ўзгаришларни бошқариш ва контрактни қайта тузиш/бузишнинг мақбул жараёнларига эга бўлиши муҳим.

Агар бегона ташкилот ўзининг сервисларини тақдим этишдан тўхтаса, у ҳолда сервисларнинг ўрнини босувчисини қидиришда тўхтаб қолишлардан мустасно бўлиш мақсадида контрактларда узлуксиз ишни таъминлаш тартиби кўзда тутилиши керак.

Бегона ташкилотлар билан тузилган контрактлар бошқа томонларни ҳам ўз ичига олиши мумкин. Учинчи томонга фойдаланишни тақдим этадиган контрактларга бошқа томонларни жалб этишга йўл қўйиш, шунингдек, уларнинг фойдаланиш ва қатнашиш шартлари киритилиши керак.

Одатда, контрактларни ташкилотнинг ўзи ишлаб чиқади. Баъзи ҳолларда контракт бегона ташкилот томонидан ишлаб чиқилган ва тақдим этилган бўлиши мумкин. Ташкилот бегона ташкилот томонидан тақдим этилаётган контрактда айтиб ўтилган талаблар томонидан ўзининг хавфсизлигига ортиқча таъсир бўлмаслигини таъминлаши зарур.

7 Активларни бошқариш

7.1 Активлар учун жавобгарлик

Мақсад: ташкилот активларининг тегишли муҳофазасини таъминлаш ва сақлаб туриш.

Барча асосий ахборот активлари ҳисобга олинган ва жавобгар эгаларига бириктирилган бўлиши керак.

Барча асосий активларнинг эгаларини идентификациялаш ва ахборот хавфсизлигини бошқариш бўйича тегишли тадбирларни таъминлаш учун уларнинг жавобгарлигини белгилаш зарур. Ахборот хавфсизлигини бошқариш бўйича тадбирларни амалга ошириш бошқага юкланиши мумкин, лекин жавобгарлик активнинг тайинланган эгасида қолиши керак.

7.1.1 Активларни инвентаризация қилиш

Бошқариш воситаси

Ташкилотнинг барча ахборот активлари аниқ белгиланган бўлиши керак, барча муҳим активларнинг рўйхати тузилиши ва доимо сақланиши керак.

Жорий этиш бўйича қўлланма

Ташкилот барча активларнинг муҳимлигини белгилаши ва ҳуж-жатлаштириши керак. Активлар реестрига авариядан кейин тиклаш учун барча ахборотни, жумладан активнинг тури, формати, жойлашиши, резервлаш, лицензиялар бўйича ахборотни ва бизнес учун қийматини киритиш керак. Ушбу реестр бошқа рўйхатларни такрорламаслиги керак, лекин унинг структураси уларга мос келиши керак.

Бундан ташқари, активларнинг ҳар бири учун эгаликни (7.1.2) келишиш ва ҳужжатлаштириш ҳамда ахборотни таснифлаш (7.2) керак. Активларнинг бизнес учун қиймати ва уларни хавфсизлик бўйича таснифи асосида активларнинг муҳимлигига мос келадиган муҳофаза қилиш даражаси белгиланиши керак (активларнинг муҳимлигини тасаввур этиш учун уларни баҳолаш бўйича бундан кейинги ахборот ISO/OEC TR 13335-3 да мавжуд).

Бошқалар

Активларнинг кўп турлари мавжуд, жумладан:

а) ахборотга оид: маълумотлар базаси ва маълумотлар файллари, контрактлар ва битимлар, тизим ҳужжатлари, тадқиқот ҳужжатлари,

фойдаланувчиларнинг қўлланмалари, ўқув материаллари, эксплуатация қилиш ёки қўллаб-қувватлаш (хизмат кўрсатиш) жараёнлари, узлуксиз ишни таъминлаш бўйича режалар, резервлаш бўйича тадбирлар, баённомалар ва архивлаштирилган ахборот;

b) дастурий таъминот активлари: амалий дастурий таъминот, тизим дастурий таъминоти, ишлаб чиқаришнинг инструментал воситалари ва утилитлар;

c) жисмоний активлар: компьютер ускунаси, телекоммуникациялар ускунаси, алмашинувчи ташувчилар ва бошқа техник ускуна;

d) хизматлар: ҳисоблаш хизматлари ва телекоммуникациялар хизматлари, масалан, иситиш, ёритиш, электр билан таъминлаш ва ҳавони кондициялаш;

e) одамлар, уларнинг малакаси, кўникмаси ва тажрибаси;

f) ташкилотнинг обрўси ва имижи каби номоддий активлар.

Активларни инвентаризация қилиш уларнинг самарали муҳофаза қилиниши таъминланаётганлигига ишонч бағишлайди, шунингдек, у бошқа бизнес-мақсадлар, меҳнат хавфсизлигини таъминлаш, суғурта ёки молиявий масалаларни ҳал қилиш (активларни бошқариш) учун талаб қилиниши мумкин. Активларни инвентаризация қилиш жараёни - хавфларни бошқаришнинг муҳим жиҳатидир (4).

7.1.2 Активларга эгалик қилиш

Бошқариш воситаси

Ахборотга ишлов бериш воситалари билан боғлиқ барча ахборот ва активлар ташкилотнинг белгиланган бўлинмасига (эгасига)[2] тегишли бўлиши керак.

Жорий этиш бўйича қўлланма

Активнинг эгаси қуйидагиларга жавобгар ҳисобланади:

a) ахборотга ишлов бериш воситалари билан боғлиқ ахборот ва активларнинг тегишли таснифланишини таъминлаш;

b) фойдаланишни бошқаришнинг амалдаги сиёсати асосида чеклашлар ва фойдаланишни таснифлашни чегаралаш ва даврий равишда қайта кўриш.

Қуйидагиларга эгалик қилиш мумкин:

a) бизнес-жараёнларга;

b) ҳаракатларнинг маълум тўпламига;

c) иловаларга;

d) маълумотларнинг маълум тўпламига.

[2] «Эга» атамаси корхонани, ишлаб чиқаришни, ёрдам кўрсатишни, активлардан фойдаланишни ва уларнинг хавфсизлигини бошқариш учун раҳбарий жавобгарликка тасдиқланган шахс ёки объектни билдиради. «Эга» атамаси шахс ҳақиқатда ҳам активга эгалик қилиш ҳуқуқига эгалигини билдирмайди.

Бошқалар

Кундалик масалалар кимгадир юкланиши мумкин, масалан, кунда активларни кузатувчи операторга, лекин жавобгарлик эгасининг зиммасида қолади.

Балки мураккаб ахборот тизимларида «сервислар» каби специфик функцияларни ифодаловчи бирга ҳаракат қилувчи активлар гуруҳини белгилаш фойдали бўлади. Бундай ҳолда сервис эгаси сервисни тақдим этиш учун жавобгар ҳисобланади, жумладан активлар ишини, унинг тақдим этувчиларини ҳисобга олганда.

7.1.3 Активлардан йўл қўйилган фойдаланиш

Бошқарш воситаси

Ахборотга ишлов бериш воситалари билан боғлиқ ахборот ва активлардан йўл қўйилган фойдаланиш қоидаларини аниқ белгилаш, ҳужатлаштириш ва жорий этиш керак.

Жорий этиш бўйича қўлланма

Барча ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчилари ахборотга ишлов бериш воситалари билан боғлиқ ахборот ва активлардан йўл қўйилган фойдаланиш қоидаларига риоя қилишлари керак, жумладан:

a) электрон почта ва Интернет тармоғидан фойдаланиш қоидалари (10.8);

b) мобил қурилмалардан фойдаланиш бўйича кўрсатмалар, айниқса улардан ташкилот ташқарисида фойдаланиш бўйича (11.7.1).

Раҳбар муайян қоидалар ёки қўлланмаларни тақдим этиши керак. Ташкилот ахборот активларидан фойдаланувчи ва фойдаланиш ҳуқуқига эга ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчилари улар томонидан фойдаланилдиган ахборотга ишлов бериш воситалари билан боғлиқ ахборот ва активлардан фойдаланишга қўйиладиган чеклашлар тўғрисида билишлари керак. Улар ахборотга ишлов бериш воситалари билан боғлиқ ахборот активларидан фойдаланиш учун, шунингдек, улар жавобгар бўлган ахборот активларидан исталган фойдаланиш учун жавобгар эканликларини билишлари керак.

7.2 Ахборотни таснифлаш

Мақсад: ахборот активларини муҳофаза қилишнинг керак даражасини таъминлаш.

Ахборотнинг устуворлиги, зарурлиги ва у билан ишлаганда унинг муҳофза қилиш даражасини аниқлаш учун уни таснифлаш керак.

Ахборот сезгирлик ва жиддийликнинг турли даражаларига эга. Ахборотнинг баъзи турлари муҳофза қилишнинг қўшимча даражасини ёки ишлов беришнинг махсус методларини талаб қилиши мумкин. Ахборотни таснифлаш тизимидан тегишли муҳофза қилишнинг кўпгина

даражаларини ва ишлов беришнинг махсус методларига бўлган эҳтиёжни аниқлаш учун фойдаланилади.

7.2.1 Таснифлашнинг асосий принциплари

Бошқариш воситаси

Ахборотни қонун ҳужжатларининг талаблари бўйича, шунингдек, аҳамияти, сезгирлиги ва ташкилот учун сезгирлиги бўйича таснифлаш керак.

Жорий этиш бўйича қўлланма

Ахборотни ва ахборот хавфсизлигини бошқариш бўйича улар билан боғлиқ тадбирларни таснифлашда биргаликда фойдаланиладиган бизнес талабларини ёки ахборотдан фойдаланишни чеклашларни, шунингдек, бизнес учун бундай талаблар билан боғлиқ оқибатларни ҳисобга олиш керак.

Таснифлаш бўйича кўрсатмалар фойдаланишни бошқаришнинг баъзи олдиндан белгиланган сиёсатларига мувофиқ дастлабки таснифлаш ва кейинги қайта таснифлаш бўйича контрактларни ўз ичига олиши керак (11.1.1).

Активнинг эгаси (7.1.2) активларни таснифлаш, уни вақти-вақти билан қайта кўриб чиқиш, шунингдек, унинг долзарблилиги ва керакли даражасини таъминлаш учун жавобгар ҳисобланади. Таснифлашда агрегирлаш самарасини ҳисобга олиш керак (10.7.2).

Ахборотни таснифлашнинг ҳаддан ташқари мураккаб схемалари фойдаланиш учун қийин ва тежамсиз ёки амалга ошириб бўлмайдиган бўлиши мумкин. Бошқа ташкилотлардан олинган ҳужжатлар грифларининг номига бошқа маъно бериши мумкин бўлган махфийлик грифини талқин қилишда эҳтиёт бўлиш керак.

Бошқалар

Муҳофаза қилиш даражасини, кўрилаётган ахборотга қўйилган конфиденциаллик, бутлик, фойдалана олиш ва ҳар қандай бошқа талабларни таҳлил қилиш ёрдамида баҳолаш мумкин.

Маълум бир вақт ўтиши билан ахборот сезгир ёки критик бўлмай қолади, масалан, агар ахборот очиқ бўлса. Ушбу масалаларни эътиборга олиш керак, чунки ҳаддан ортиқ таснифлаш бошқаришнинг керак бўлмаган воситаларини амалга оширишга олиб келиши мумкин, бу эса, қўшимча сарф-харажатларга олиб келади.

Таснифлаш даражасини белгилашда хавфсизликнинг шунга ўхшаш талаблари бўлган ҳужжатларни биргаликда кўриб чиқиш таснифлаш масаласини осонлаштириши мумкин.

Умуман ахборотни таснифлаш ушбу ахборотдан қандай фойдаланиш ва уни қандай муҳофаза қилишни белгилашнинг энг тез усули ҳисобланади.

7.2.2 Ахборотни маркалаш ва унга ишлов бериш

Бошқариш воситаси

Ташкилот томонидан қабул қилинган таснифлаш тизимига мувофиқ ахборотга ишлов беришда ахборотни маркалаш учун процедураларнинг тегишли тўпламини аниқлаш ва жорий этиш керак.

Жорий этиш бўйича қўлланма

Маркалаш процедуралари жисмоний ҳамда электрон шаклда тақдим этилган ахборот активларига тааллуқли бўлиши керак

Конфиденциал ёки сезгир каби таснифланган ахборотни ўз ичига олган маълумотларни тизимлардан чиқариш амалга оширилганда тегишли махфийлик грифидан фойдаланиш керак. Маркалашда таснифлаш даражасини акс эттириш керак (7.2.1). Босиб чиқарилган ҳисоботларни, экран шаклларини, ахборот ташувчилари (ленталар, дисклар, компакт-дисклар, кассеталар)ни, электрон хабарларни ва узатиладиган файлларни маркалаш керак.

Таснифлашнинг ҳар бир даражаси учун ишлаш, жумладан хавфсиз ишлов бериш, сақлаш, узатиш деклассификация қилиш ва йўқ қилиш тартибини белгилаш керак. Шунингдек, «етказиб бериш кетма-кетлиги» процедураларини киритиш ва хавфсизликка тегишли ҳар қандай воқеаларни журналда қайд этиш керак.

Ахборотдан биргаликда фойдаланишни кўзда тутган бошқа ташкилотлар билан тузилган битимлар берилган ахборотни таснифлашни белгилаш ва бошқа ташкилотнинг таснифлаш белгиларини талқин қилиш тартибини ўз ичига олиши керак.

Бошқалар

Маркалаш ва таснифланган ахборотдан хавфсиз фойдаланиш ахборотдан биргаликда фойдаланиш бўйича контрактларга қўйилган асосий талаб ҳисобланади. Маркалашнинг одатдаги шакли жисмоний белги ҳисобланади. Бироқ, баъзи электрон кўринишдаги ҳужжатлар каби ахборот активларини жисмоний маркалаб бўлмайди, шунинг учун электрон воситалардан, масалан экранларда ёки дисплейларда пайдо бўлиши мумкин бўлган хабар берувчи белгилардан фойдаланиш зарур. Маркалашдан фойдаланиш мақсадга мувофиқ бўлмаган ҳолларда, ахборотни таснифлаш даражасини белгилашнинг бошқа воситалари қўлланиши мумкин, масалан процедуралар ва метамаълумотлар.

8 Ходимларнинг хавфсизлиги

8.1 Ишга жойлашгунча[3]

Мақсад: ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчилари ўз мажбуриятларини тушунишлрига ва эгаллаб турган лавозимларига мос келишларига ишонч ҳосил қилиш, шунингдек, ўғирлик, фирибгарлик, майда ўғирлик ёки ахборотга ишлов бериш воситаларидан нотўғри фойдаланиш каби инсоний омил билан боғлиқ хатолардан келиб чиққан хавфларни минимумга келтириш.

Хавфсизлик билан боғлиқ жиҳатларни ходимларни олиш босқичидаёқ ҳисобга олиш, уларни меҳнат шартномаларига, лавозим йўриқномаларига киритиш, шунингдек, ходимнинг ишлаш даври мобайнида назорат қилиш керак.

Ишга жойлашишни истаган барча даъвогарлар, субпудратчилар ва бегона ташкилотлар фойдаланувчиларини тегишли тарзда текшириш керак, бу айниқса, конфиденциал ахборотдан фойдаланиш кўзда тутилаётган лавозимларга тегишли.

Ташкилотнинг ахборотга ишлов бериш воситаларидан фойдаланувчи ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчилари конфиденциаллик ва ошкор қилмаслик тўғрисидаги контрактни имзолашлари керак.

8.1.1 Мажбуриятлар ва жавобгарлик

Бошқариш воситаси

Ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчиларининг мажбуриятлари ва жавобгарлигини ташкилот ахборот хавфсизлигининг сиёсатига мувофиқ барча зарур бўлган жойларда ҳужжатлаштириш керак.

Жорий этиш бўйича қўлланма

Ахборот хавфсизлиги бўйича мажбуриятлар ва жавбгарлик қуйидаги талабларни ўз ичига олиши керак:

a) ташкилот ахборот хавфсизлигининг сиёсатига мувофиқ амалга оширишлар ва хатти-ҳаракатлар (5.1);

b) ахборот активларини рухсатсиз фойдаланишдан, уларни ошкор қилиш, ўзгартириш, йўқ қилиш ва уларга аралашишдан муҳофаза қилиш;

c) хавфсизлик бўйича алоҳида жараён ва хатти-ҳаракатларни бажариш;

d) қабул қилинаётган шахснинг мажбуриятларини белгилаб бериш;

[3] «Ишга жойлашиш» деганда, бу ерда қуйидагича турли вазиятларни тушуниш керак: одамларнинг ишга жойлашиши (вақтинчалик ёки узоқ муддатга), лавозимларга тайинлашлар ва бошқа лавозимга ўтказишлар, контрактларни тузиш, шунингдек, санаб ўтилган тадбирлардан исталганининг амал қилишини тўхтатиш.

e) хавфсизлик воқеалари, хавфсизликнинг потенциал воқеалари ёки хавфсизликнинг бошқа хавфлари тўғрисида ҳисобот бериш.

Хавфсизлик бўйича мажбуриятлар ва жавбгарлик аниқ белгиланган ва лавозим даъвограларига меҳнат шартномаси тузилмасидан олдин маълумот учун етказилган бўлиши керак.

Бошқалар

Хавфсизлик бўйича мажбуриятлар ва жавбгарликни ҳужжатлаштириш учун лавозим йўриқномаларидан фойдаланиш мумкин. Шунингдек, ташкилот билан меҳнат шартномасини тузиш жараёнида қатнашмайдиган, масалан, бегона ташкилот ёрдамида ишлайдиган шахсларга хавфсизлик бўйича мажбуриятлар ва жавобгарликни аниқ белгилаш ва тушунтириш керак.

8.1.2 Танлов

Бошқариш воситаси

Ишга жойлашишни истаган барча даъвогарлар, субпудратчилар ва бегона ташкилотлар фойдаланувчилари таржимаи ҳолларининг назорат текширувларини қонун ҳужжатлари, нормалар, этика ва бизнес талаблари, фойдаланилишга мансуб ахборотни таснифлаш талабларига мутаносиб равишда, шунингдек, қабул қилинадиган хавфларга мувофиқ амалга ошириш керак.

Жорий этиш бўйича қўлланма

Назорат текширувларини ўтказишда шахсий маълумотларнинг конфиденциаллигини таъминлаш ва муҳофаза қилинишини, ишга жойлашиш тўғрисидаги қонун ҳужжатлари бўйича барча тегишли чораларни эътиборга олиш керак, шунингдек, рухсат мавжудлигида текширувлар қуйидагиларни ўз ичига олиши керак:

a) ижобий тавсияларнинг мавжудлиги, хусусан, даъвогарнинг ишчанлик ва шахсий фазилатларига тегишли;

b) даъвогар тўғрисидаги қисқа маълумотлар (тўлиқлиги ва аниқлиги)ни текшириш;

c) эълон қилинган маълумоти ва касбий малакасининг тасдиғи;

d) шахсини тасдиқловчи ҳужжат (паспорт ёки унинг ўрнини босувчи ҳужжат)ларнинг ҳақиқийлигини мустақил текшириш;

e) кредит карталарни ва судланганликни текшриш каби батафсилроқ текширувлар.

Агар ишга қабул қилинганидан сўнг ёки қабул қилиш жараёнида янги ходимнинг конфиденциал ахборотга, масалан, ташкилотнинг молиявий ёки ўта махфий ахборотига ишлов бериш воситаларидан фойдаланишига тўғри келиб қолса, махсус текширув амалга оширилиши керак.

Процедураларда махсус текширувлар учун мезонлар ва чеклашлар белгиланиши керак, масалан, ким танловни бажариш ҳуқуқига эга, шунингдек, махсус текширувлар қандай, қачон ва нима учун бажарилиши.

Шунингдек, субпудратчилар ва бегона ташкилотлар фойдаланувчилари учун танлов жараёни қўлланиши керак.

Субпудратчиларни қабул қилиш кадрлар агентлиги орқали амалга оширилган ҳолларда, агар текширув тугамаган ва унинг натижалари танланган даъвогардан шубҳаланиш ва ҳавотирланишга асос бўлса, агентлик билан тузилган контракт агентлик амал қилиши керак бўлган даъвогарларни текшириш ва уларни хабардор қилиш процедуралари бўйича агентликнинг мажбуриятларини аниқ белгилаб бериши керак. Бегона ташкилотлар билан тузилган контрактларда барча мажбуриятлар ва танловда хабардор қилиш тартиби худди шундай тарзда аниқ баён этилган бўлиши керак (6.2.3).

Ташкилот ичидаги лавозимлар учун кўриб чиқилаётган барча даъвогарлар бўйича ахборотни керак нормалар ва амалдаги қонун ҳужжатларига мувофиқ йиғиш ва унга ишлов бериш керак.

Қўлланадиган нормаларга қараб даъвогарларни танлов бўйича тадбирлар тўғрисида олдиндан хабардор қилиш керак.

8.1.3 Меҳнат шартномасининг шартлари

Бошқариш воситаси

Ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчилари меҳнат шартномасининг шартларига, ўзларининг шартнома мажбуриятларининг қисми сифатида рози бўлганларида уни имзолайдилар. Шартномада ушбу шахслар ва ташкилотнинг ахборот хавфсизлиги бўйича мажбуриятлари ифодаланган бўлиши керак.

Жорий этиш бўйича қўлланма

Меҳнат шартномасининг шартларида ахборот хавфсизлиги сиёсатини акс эттиришдан ташқари қуйидагиларни ёритиш ва ифодалаш керак:

a) конфиденциал ахборотдан фойдаланишга рухсат этилган барча ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчиларига ахборотга ишлов бериш воситаларидан фойдаланишга рухсат беришдан олдин конфиденциаллик ёки ошкор этмаслик тўғрисида контракт имзоланиши керак;

b) ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчиларининг қонуний ҳуқуқлари, масалан, муаллифлик ҳуқуқи ёки маълумотларни муҳофаза қилиш тўғрисидаги қонун ҳужжатларига тегишли (15.1.1, 15.1.2);

c) ахборотни таснифлаш ва ходимлар, субпудратчилар ёки бегона ташкилотларнинг фойдаланувчилари мурожаат қиладиган ахборот тизимлари ва сервислари билан боғлиқ ташкилот активларини бошқариш бўйича мажбуриятлар (7.2.1, 10.7.3);

d) ходимлар, субпудратчилар ёки бегона ташкилотлар фойдаланувчиларининг бошқа компаниялар ёки бегона ташкилотлардан олинадиган ахборотдан фойдаланиш бўйича мажбуриятлари;

e) шахсий ахборотдан фойдаланиш қоидалари, жумладан ташкилот билан меҳнат шартномасини тузиш натижаси ёки жараёнида яратилган шахсий ахборотдан (15.1.4);

f) ташкилотдан ташқарида ва ишдан ташқари вақтда, масалан, касаначиликда бажарилиши зарур бўлган мажбуриятлар (9.2.5, 11.7.1);

g) ходимлар, субпудратчилар ёки бегона ташкилотлар фойдаланувчилари томонидан ташкилот хавфсизлиги талаблари инобатга олинмаган ҳолларда кўриладиган чоралар.

Ташкилот ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчилари ушбу шахсларга ахборот тизимлари ва сервислари билан боғлиқ ташкилот активларидан фойдаланишнинг тақдим этиладиган фойдаланиш тури ва даражасига мувофиқ ахборот хавфсизлигига тегишли шартларга розиликларига ишонч ҳосил қилиши керак.

Зарурат бўлганда, жавобгарлик меҳнат муносабатлари тугатилганидан сўнг ҳам маълум муддат давомида сақланиши керак (8.3).

Бошқалар

Ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчиларининг конфиденциаллик, маълумотларни муҳофаза қилиш, этика, ташкилот ускунасидан тўғри фойдаланишга, шунингдек, ташкилот томонидан кутилган муносиб ахлоққа тааллуқли мажбуриятларини таърифлаш учун ахлоқ кодексидан фойдаланиш мумкин. Субпудратчилар ва бегона ташкилотлар фойдаланувчилари ўз навбатида ёлланган ходим номидан шартнома муносабатлари ўрнатилиши талаб қилиниши мумкин бўлган ташқи ташкилот билан алоқада бўлишлари мумкин.

8.2 Ишга жойлашиш даврида

Мақсад: ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчилари ахборот хавфсизлиги билан боғлиқ таҳдид ва муаммолар тўғрисида хабардор қилинганликлари, шунингдек, ўз хизмат мажбуриятларини бажаришда оддий иш мойбайнида ва «инсон омили» натижасида хато қилиш хавфлари юзага келган ҳолларда ташкилот хавфсизлигининг сиёсати талабларига риоя қилиш билан боғлиқ процедураларни бажариш учун зарур кўникмаларга эга эканликларига ишонч ҳосил қилиш.

Даъвогарнинг ташкилот ичида ишга жойлашиши даврида раҳбариятнинг хавфсизлик чораларини таъминлаш бўйича мажбуриятларини белгилаш керак.

Хавфсизликнинг мумкин бўлган хавфларини минимумга келтириш учун барча ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчиларининг хавфсизлик процедуралари ва ахборотга ишлов бериш воситаларидан тўғри фойдаланиши бўйича етарли хабардорлик, ўқитиш ва тренингларни таъминлаш керак. Хавфсизликнинг бузилишларига ишлов беришнинг расмий интизомий жараёнини тасдиқлаш керак.

8.2.1 Раҳбариятнинг мажбуриятлари

Бошқариш воситаси

Раҳбарият ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчиларидан ташкилотнинг тасдиқланган сиёсатлари ва процедураларига мувофиқ керакли тарзда хавфсизликка муносабат билдиришларини талаб қилиши керак.

Жорий этиш бўйича қўлланма

Ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчилари:

a) уларга конфиденциал ахборот ёки ахборот тизимларидан фойдаланиш учун рухсат берилгунча ўзларининг ахборот хавфсизлиги бўйича лавозим мажбуриятлари тўғрисида керакли тарзда йўл-йўриқлар олган бўлишлари;

b) уларнинг ташкилот ичидаги вазифаларига тегишли хавфсизлик бўйича кўрсатмалар олишлари;

c) ташкилот хавфсизлиги сиёсатини бажариш асосланган бўлиши;

d) уларнинг ташкилотдаги лавозим мажбуриятларига тегишли хабардорлик даражасига етишлари (8.2.2);

e) меҳнат шартномаси шартларига ва ташкилот ахборот сиёсатига, шунингдек, фаолиятнинг қабул қилса бўладиган методларига риоя қилишлари;

f) керакли кўникма ва маҳоратга эга бўлишлари учун раҳбарият чора-тадбирлар кўриши керак.

Бошқалар

Агар ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчиларига уларнинг хавфсизлик бўйича жавобгарлиги тўғрисида хабар берилмаса, улар ташкилотга катта зарар келтиришлари мумкин. Эҳтимол, ишончни оқлаган ходим энг ишончли ва ахборот хавфсизлигида инцидентларни кам чақирувчи ходим ҳисобланади.

Раҳбариятнинг талабчан бўлмаслиги ходимда ташкилот хавфсизлигига таъсир қилувчи қадрламаслик туйғусини юзага келишига сабаб бўлиши мумкин. Масалан, бундай раҳбарлик хавфсизликка аҳамият бермасликка ёки ташкилот активларининг мақсадсиз потенциал фойдаланилишига олиб келиши мумкин.

8.2.2 Ходимларни хавфсизлик қоидаларига ўқитиш

Бошқариш воситаси

Ташкилотнинг барча ходимлари, зарур бўлган жойларда эса, субпудратчилар ва бегона ташкилотларнинг фойдаланувчилари ҳам тегишли билим олишлари ва ташкилотда қабул қилинган ва уларнинг лавозим мажбуриятларига тегишли ахборот хавфсизлиги сиёсатлари ва процедураларининг янгиланган вариантларини мунтазам олиб туришлари керак.

Жорий этиш бўйича қўлланма

Ахборотдан ёки сервердан фойдаланиш тақдим этилгунча ахборот хавфсизлигининг сиёсати ва уни бажаришнинг кутилаётган натижалари билан таништириш мақсадида тренинг ўтказилиши керак.

Тренинг жараёнида хавфсизлик талабларини, юридик жавобгарлик ва бизнесни бошқариш воситаларини, ахборотга ишлов бериш воситаларидан тўғри фойдаланишни, масалан, тизимларда рўйхатга олиш процедураларини, дастурлар пакетидан, шунингдек, интизомий чоралар тўғрисидаги ахборотдан фойдаланишни кўриб чиқиш керак (8.2.3).

Бошқалар

Ходимнинг хавфсизлик соҳасидаги хабардорлиги, ўқитилиши ва тренинглар бўйича тадбирлар мақбул бўлиши ва фойдаланувчининг лавозимига, мажбуриятлари ва кўникмаларига мос келиши, шунингдек, маълум таҳдидлар, хавфсизлик бўйича маслаҳат учун кимга мурожаат қилиниши ва ахборот хавфсизлиги инцидентлари тўғрисида кимга хабар берилиши бўйича ахборотни ўз ичига олиши керак (13.1).

Фойдаланувчиларнинг хабардорлигини ошириш бўйича тренинг аниқ мисоллар ёрдамида ахборот хавфсизлигининг мумкин бўлган муаммолари ва инцидентларини, уларга муносабат билдириш усулларини, шунингдек, улар тўғрисида хабар беришнинг белгиланган тартибини намойиш этишга имкон беради.

8.2.3 Интизомий чоралар

Бошқариш воситаси

Ташкилот хавфсизлик сиёсатини ва процедураларини бузган ходимнинг интизомий чораларини белгилаб берадиган расмий процедуралар мавжуд бўлиши керак.

Жорий этиш бўйича қўлланма

Олдиндан текширмасдан ва хавфсизлик бузилганлигига аниқ ишонч ҳосил қилмасдан туриб интизомий жараённи бошлаш керак эмас (13.2.3).

Расмий интизомий жараёнда хавфсизликнинг бузилишида гумон қилинаётган ходимга нисбатан объектив ва адолатли муомала қилиниши таъминланиши керак. Расмий интизомий жараён бузилишнинг табиати ва жиддийлиги каби омилларни, унинг бизнесга таъсири, ушбу бузилиш биринчими ёки рецидивми, қоида бузувчи керакли тарзда йўриқнома олганми йўқми, қонун ҳужжатларига, хизматга оид контрактлар ва бошқа зарур омилларни ҳисобга оладиган дифференциация қилинган муносабатни таъминлаши керак. Жиддий хатоларда жараён фойдаланиш мажбуриятлари, ҳуқуқлари ва имтиёзларидан дарҳол маҳрум этилишига, зарур бўлганда эса, кечиктирмасдан объектдан чиқариб юборилишига йўл қўйиши керак.

Бошқалар

Интизомий жараёндан хавфсизлик сиёсати ва процедуралари бузилишининг, шунингдек, ходимлар, субпудратчилар ва бегона

ташкилотлар фойдаланувчилари томонидан бошқа ҳар қандай бузилишларнинг олдини олиш учун восита сифатида фойдаланиш керак.

8.3 Меҳнат шартномасини тўхтатиш ва бошқа лавозимга ўтказиш тартиби

Мақсад: ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчиларининг меҳнат шартномасини тўхтатиш ва бошқа лавозимга ўтказиш тартибини таъминлаш.

Ходимнинг меҳнат шартномасини тўхтатиш, субпудратчилар ва бегона ташкилотлар фойдаланувчиларини ташкилотдан кетиши, шунингдек, ташкилотга тегишли барча ускунани қайтариш ва ишдан бўшатилганларнинг барча фойдаланиш ҳуқуқларини йўқ қилиш тартиби бўйича мажбуриятлар баён этилиши керак.

Ташкилот билан меҳнат шартномасини имзолаш тартиби ўзгаришига меҳнат шартномасининг ушбу бўлимга мувофиқ бекор қилиниши каби қараш керак. Меҳнат шартномасининг ҳар қандай янги имзоланишига 8.1-бандда баён этилганидек муносабат билдириш керак.

8.3.1 Меҳнат шартномасини тўхтатиш

Бошқариш воситаси

Меҳнат шартномасини тўхтатиш ва бошқа лавозимга ўтказиш тартибини аниқ белгилаш керак.

Жорий этиш бўйича қўлланма

Меҳнат шартномасини тўхтатиш тартиби хавфсизликнинг амалдаги талабларини, юридик асосланганликни ва жавобгарликни, зарурат бўлганда эса, конфиденциаллик тўғрисидаги контрактга (6.1.5) киритилган мажбуриятларни ва ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчилари билан меҳнат шартномасининг амал қилиши тугатилганидан сўнг (8.1.3) маълум муддатга тааллуқли меҳнат шартномасининг шартларини ўз ичига олиши керак.

Меҳнат шартномасининг амал қилиши тугатилганидан сўнг амал қиладиган жавобгарлик ва мажбуриятларни ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчилари билан янгитдан тузиладиган контрактларга киритиш керак.

Меҳнат шартномасининг ўзгариши ва бошқа лавозимга ўтишга меҳнат шартномасининг тўхтатилиши каби қараш керак; янги мажбуриятларни ва меҳнат шартномасини бошқариш керак (8.1).

Бошқалар

Кадрлар бўлими, одатда, меҳнат шартномасини тўхтатиш жараёнига жавоб беради ва тегишли процедураларнинг хавфсизлигини бош-қариш учун ишдан бўшатилаётган ходимнинг раҳбари билан бевосита ҳамкорлик қилади. Субпудратчи билан бундай ҳол юз берганда ушбу мажбуриятларни тўхтатиш жараёни субпудратчи учун жавобгар агентлик

томонидан, бошқа фойдаланувчилар билан бўлган ҳолатда эса, уларнинг ташкилотлари томонидан бажарилиши мумкин.

Имкони борича ходимлар, мижозлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчиларини ходимлар ва ишчиларни бошқа лавозимга ўтказиш тўғрисида хабардор қилиш керак.

8.3.2 Активларнинг қайтарилиши

Бошқариш воситалари

Барча ходимлар, субпудратчилар ва бегона ташкилотлар фойдаланувчиларининг меҳнат шартномалари, контрактлари ёки контрактларининг амал қилиш муддати тугаганида уларда бўлган барча активлар ташкилотга қайтарилиши керак.

Жорий этиш бўйича қўлланма

Меҳнат шартномасини тўхтатиш жараёнини расмийлаштириш ва аввал берилган дастурий таъминот, корпоратив ҳужжатлар ва ускунанинг қайтарилишини таъминлаш керак. Шунингдек, ташкилотнинг мобил ҳисоблаш қурилмалари, кредит карталари, фойдаланиш карталари, йўриқномалар ва электрон ташувчилардаги йўриқнома ва ахборот каби бошқа активлари ҳам қайтарилиши керак.

Ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчилари ташкилот ускунасини сотиб олган ёки шахсий ускунадан фойдаланган ҳолларда барча зарур ахборотни кўчириш ва унинг ушбу ускунадан ишончли йўқ қилинишини таъминловчи процедураларга риоя қилиниши керак (10.7.1).

Ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчиларида операциянинг ҳозирги вақти учун муҳим билимлари бўлганда, ушбу ахборотни ҳужжатлаштириш керак.

8.3.3 Фойдаланиш ҳуқуқини олиб қўйиш

Бошқариш воситаси

Ходимлар, субпудратчилар ёки бегона ташкилотлар фойдаланувчиларининг ахборот ва унга ишлов бериш воситаларидан фойдаланиш ҳуқуқларини меҳнат шартномаси, контракти, контрактининг амал қилиш муддати тугаганидан сўнг олиб қўйиш керак. Бошқа лавозимга ўтказишда фойдаланиш ҳуқуқи ўзгартирилиши зарур.

Жорий этиш бўйича қўлланма

Меҳнат шартномаси тугатилганда фойдаланувчиларнинг ахборот тизимлари ва сервисларига тегишли активларидан фойдаланиш ҳуқуқини қайта кўриб чиқиш керак. Бунда фойдаланиш ҳуқуқларини олиб қўйиш зарурати аниқланади. Ходимнинг лавозимини ўзгартириш муносабати билан унга аввалги жойида тақдим этилган барча ҳуқуқлар олиб қўйилади. Олиб қўйилиши керак бўлган фойдаланиш ҳуқуқлари ўз ичига жисмоний ва мантиқий фойдаланишни, калитларни, идентификацион карталарни, ахборотга ишлов бериш воситаларини (11.2.4), гувоҳномаларни олади, шунингдек, ишдан бўшатилаётган ходимни ташкилот ходими сифатида

тан оладиган ҳар қандай ҳужжатларнинг ёзувларидан ўчириш амалга оширилади. Агар кетаётган ходим, субпудратчи ёки бегона ташкилот фойдаланувчисининг ҳисобга олиш паролларидан хабардор бўлса, актив бўлиб қоладиган ушбу паролларни ишдан бўшатишда ёки иш жойини, контракт ёки контрактни ўзгартиришда ўзгартириш керак.

Ахборот активлари ва ахборотга ишлов бериш воситаларидан фойдаланиш ҳуқуқи қуйидагилар каби хавфлар омилларини баҳолашга боғлиқ ҳолда меҳнат шартномаси тугатилгунича ёки ўзгартирилгунича чеклаш ёки олиб қўйиш керак:

a) ходимни ишдан бўшатиш ёки лавозимини ўзгартириш, шунингдек, ишдан бўшатиш сабаблари ходим, субпудратчи ёки бегона ташкилотнинг фойдаланувчиси ёҳуд раҳбарият томонидан инициация қилинганлиги;

b) ходим, субпудратчи ёки ҳар қандай бошқа фойдаланувчининг кундалик мажбуриятлари;

c) ҳозирги вақтда фойдаланиш мумкин бўлган активларнинг аҳамияти.

Бошқалар

Маълум шароитларда фойдаланиш ҳуқуқидан ходим, субпудратчи ёки бегона ташкилотларнинг фойдаланувчисидан ташқари, бошқа шахслар фойдаланиши мумкин, масалан гуруҳли идентификаторлар. Бундай шароитларда ишдан бўшатилаётганлар тўғрисидаги маълумотларни гуруҳли фойдаланишнинг ҳар қандай рўйхатларидан ўчириш керак ва барча ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчиларига ишдан бўшатилаётган фойдаланувчи билан ахборот активларидан биргаликда фойдаланишни тақдим этишни ман этиш тўғрисида хабар бериш керак.

Меҳнат шартномаси раҳбарнинг ташаббуси билан тўхтатилган ҳолда норози ходим, субпудратчилар ёки бегона ташкилотларнинг фойдаланувчилари атайлаб ахборотга шикаст етказишлари ва унга ишлов бериш воситаларини тўхтатиб қўйишлари мумкин. Шахсларни қайта тайинлаш ҳолларида улар кейинчалик фойдаланиш учун ахборот йиғишга уринишлари мумкин.

9 Жисмоний хавфсизлик ва атроф-муҳит хавфсизлиги

9.1 Қўриқланадиган зоналар

Мақсад: рухсатсиз жисмоний фойдаланиш ва ишлаб чиқариш хоналарига зарар етказишни, шунингдек, ташкилотнинг конфиденциал ахборотидан рухсатсиз фойдаланиш, уни йўқ қилиш ва бузишнинг олдини олиш.

Сезгир ёки конфиденциал ахборотга ишлов бериш воситаларини хавфсизликнинг тегишли муҳофаза тўсиқлари ва киришнинг назорат

воситалари билан жиҳозланган хавфсизлик периметри билан белгиланган хавфсизлик зонасида жойлаштириш зарур. Бу зоналар рухсатсиз фойдаланиш, шикастланиш ва халақитдан жисмоний муҳофазаланган бўлиши керак.

Муҳофазаланганлик даражаси идентификацияланган хавфлар билан мутаносиб бўлиши керак.

9.1.1 Қўриқланадиган зонанинг периметри

Бошқариш воситаси

Ахборот ва унга ишлов бериш воситалари жойлашган зоналарни жисмоний муҳофаза қилиш учун хавфсизлик периметрини қўллаш керак (тўсиқлар, карточкалар ва пропускалардан фойдаланиладиган ўтказиш пунктлари, қабулхоналар).

Жорий этиш бўйича қўлланма

Зарур бўлганда хавфсизликнинг физик периметрини жиҳозлаш бўйича қуйидаги тавсияларни кўриб чиқиш ва жорий этиш зарур:

a) хавфсизлик периметрини аниқ белгилаш керак; периметрнинг ҳар бир участкасини жойлаштириш ва унинг маҳкамлиги хавфсизликнинг периметр ичида активга бўлган талабларига ва хавфларни аниқлаш натижаларига боғлиқ бўлиши керак;

b) ахборотга ишлов бериш воситалари жойлашган бино ёки хоналар периметри жисмоний туташ бўлиши керак (яъни периметрлар ёки жойлар орасида ҳеч қандай осон ўтиб бўладиган оралиқлар бўлиши керак эмас). Хоналарнинг ташқи деворлари пишиқ конструкцияга эга бўлиши, барча ташқи эшиклар эса, етарли даражада рухсатсиз фойдаланишдан шлакбаумлар, сигнализация, қулфлар ва ш.к. билан муҳофаза қилинган бўлиши керак. Ходимлар йўқлигида эшиклар ва деразалар берк бўлиши керак, шунингдек, деразаларни ташқаридан муҳофаза қилишни кўзда тутиш керак, айниқса биринчи қаватда;

c) келувчиларни рўйхатга олиш зонаси ходим томонидан ажратилган ва комплектланган бўлиши ёки хона ёки бинога жисмоний киришни бошқариш бўйича бошқа воситалар мавжуд бўлиши керак. Хона ва бинога кириш ҳуқуқи фақат авторизация қилинган ходимга тақдим этилиши керак;

d) рухсатсиз жисмоний кириш ва атроф-муҳитни ифлослантиришнинг олдини олиш учун зарур бўлганда жисмоний тўсиқлар қурилиши керак;

e) регионал, миллий ва халқаро стандартларга мувофиқ муҳофаза қилишнинг талаб қилинган даражасини таъминлаш учун хавфсизлик периметри бўйича барча чиқишлар ва деворларни назорат қилиш ва текшириш мумкин бўлган авария сигнализацияси билан жиҳозлаш керак; авария ҳолатида қўшимча чиқишларнинг жиҳозланиши ёнғин хавфсизлиги бўйича йўриқномага мос бўлиши керак;

f) барча ташқи эшикларни ва осон очиб кириладиган деразаларни қўриқлаш учун бузғунчиларни аниқлашнинг регионал, миллий ёки

халқаро стандартларга мос келадиган тизимлари ўрнатилиши керак, уларни вақти-вақти билан текшириб туриш керак. Одам кам бўлган қўриқланадиган участкаларда сигнализация кечаю кундуз ёқиб қўйилган бўлиши керак, шунингдек, бошқа участкаларнинг, масалан, компьютер хоналари ёки оператор хоналарининг қўриқланишини таъминлаш керак;

g) ташкилот томонидан бошқариладиган ахборотга ишлов бериш воситаларини бегона ташкилот томонидан бошқариладиган ахборотга ишлов бериш воситаларидан жисмонан ажратиш керак.

Бошқалар

Жисмоний муҳофаза ташкилот хоналари ва ахборотга ишлов бериш воситалари атрофида битта ёки ундан ортиқ жисмоний тўсиқларни яратиш билан таъминланиши мумкин. Бир нечта тўсиқлардан фойдаланиш қўшимча муҳофазани таъминлайди, бунда битта тўсиқнинг бузилиши хавфсизликни дарҳол компрометация қилинишини англатмайди.

Муҳофаза қилинадиган участка физик хавфсизликнинг узлуксиз ички тўсиғи билан ўралган қулфланадиган хона ёки бир неча хонадан иборат бўлиши мумкин. Хавфсизлик периметри ичида турли хавфсизлик талабларига эга бўлган участкалар ўртасида жисмоний киришни бошқариш учун қўшимча тўсиқлар ва периметрлар керак бўлиб қолиши мумкин.

Бир неча ташкилотлар жойлашган жойларда жисмоний киришнинг хавфсизлиги бўйича махсус чоралар қабул қилиниши керак.

9.1.2 Қўриқланадиган зоналарга киришни бошқариш

Бошқариш востаси

Қўриқланадиган зоналарни фойдаланиш фақат авторизация қилинган ходимга рухсат берилганлигига ишонч ҳосил қилиш учун киришни назорат қилишнинг тегишли чоралари ёрдамида муҳофаза қилиш зарур.

Жорий этиш бўйича қўлланма

Назоратнинг қуйидаги чораларини кўриб чиқиш зарур:

a) хавфсизлик зоналарининг келувчилари кузатиб қўйилиши ёки тегишли фойдаланишга эга бўлишлари керак, уларнинг кириш ва чиқиш санаси ва вақти рўйхатга олиниши керак. Фойдаланиш фақат муайян авторизация қилинган масалаларни ечиш учун тақдим этилиши керак. Келувчиларни хавфсизлик талаблари ва авария вазиятларидаги хатти-ҳаракатлар билан таништириш керак;

b) конфиденциал ахборот ва унга ишлов бериш воситаларидан фойдаланиш назорат қилиниши ва фақат авторизация қилинган шахсларга тақдим этилиши керак. Аутентификация қилиш воситаларидан, масалан, авторизация қилиш ва тегишли фойдаланишни тақдим этиш учун фойдаланиш карталари ва бунга қўшимча шахсий идентификацион рақамнинг кодидан (PIN - код) фойдаланиш керак. Фойдаланишни рўйхатга олиш журналларининг аудитини керак тарзда ўтказиш зарур;

c) барча ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчилари кўринадиган идентификациялаш белгиларини тақиб юришларини талаб қилиш, шунингдек, уларнинг идентификациялаш карталарига эга бўлмаган ходимларга, кузатувчисиз нотаниш келувчиларга бўлган эътиборларини рағбатлантириш зарур, бу тўғрида улар хавфсизлик хизмати ходимларини дарҳол хабардор қилишлари керак;

d) бегона ташкилотларнинг қўллаб-қувватлаш хизмати ходимларига фақат зарурат бўлгандагина, муҳофазаланган участкалардан ёки конфиденциал ахборотга ишлов бериш воситаларидан чекланган фойдаланиш тақдим этилиши керак; ушбу фойдаланиш рухсат берилган ва назорат қилинадиган бўлиши керак;

e) муҳофазаланган участкалардан фойдаланиш ҳуқуқини вақти-вақти билан кўриб чиқиш ва янгилаб туриш, шунингдек, зарур бўлганда қайтариб олиш керак.

9.1.3 Бинолар, ишлаб чиқариш хоналари ва ускуналар хавфсизлиги

Бошқариш воситаси

Ишлаб чиқариш хоналари ва ускуналар учун жисмоний муҳофаза қилишни ишлаб чиқиш ва жорий этиш керак.

Жорий этиш бўйича қўлланма

Ишлаб чиқариш хоналари ва ускуналарни муҳофаза қилиш учун қуйидаги тавсияларни кўриб чиқиш керак:

a) хавфсизлик техникаси ва меҳнат муҳофазаси бўйича тегишли нормалар ва стандартларни эътиборга олиш зарур;

b) асосий ускуна бегона кишилар кириши чекланган жойларда жойлаштирилган бўлиши керак;

c) бинолар умумий фондан ажралиб турмаслиги ва ўз вазифаларининг минимал белгиларига эга бўлиши керак. Улар бинонинг ичида ёки ташқарисида кўриниб турадиган ахборотга ишлов бериш функциялари тўғрисида хулоса қилиш мумкин бўлган пешлавҳага эга бўлмаслиги керак;

d) каталоглардан ва ички телефонлар рўйхатларидан, ахборотга ишлов бериш ёпиқ воситалари жойлашган жойлар белгиланган китоблардан бегоналар осон фойдалана олмасликлари керак.

9.1.4 Ташқи ва экологик таҳдидлардан муҳофаза қилиш

Бошқариш воситаси

Ёнғин, сув тошқини, ер қимирлаши, портлаш кўчалардаги тартибсизликлар ва фавқулодда вазиятларнинг бошқа шаклларидан жисмонан муҳофаза қилишни ишлаб чиқиш ва жорий этиш керак.

Жорий этиш бўйича қўлланма

Хавфсизликнинг қўшни бинолардан бўлиши мумкин бўлган ҳар қандай таҳдидларини кўриб чиқиш керак, масалан қўшни бинода ёнғин, томдан чакка ўтиши ёки подвалдан сув тошиши, ёхуд кўчадаги портлаш.

Ёнғин, сув тошқини, ер қимирлаши, портлаш, кўчалардаги тартибсизликлар ва фавқулодда вазиятларнинг бошқа шаклларидан келадиган зарарнинг олдини олиш учун қуйидаги тавсияларни кўриб чиқиш зарур:

a) хавфли ёки ёнадиган мойлаш материалларининг ахборот хавфсизлиги зонасидан керакли масофада ишончли сақланишини таъминлаш керак. Босиб чиқарадиган қурилмалар учун қоғознинг катта захираларини ёнғин хавфсизлигининг тегишли чораларига риоя қилмасдан хавфсизлик зонасида сақлаш керак эмас;

b) резерв ускуна ва резерв нусхалар сақланадиган ахборот ташувчиларни асосий бинода фавқулодда ҳодисалар оқибатларидан шикастланишига йўл қўймаслик учун хавфсиз масофада жойлаштириш керак;

c) ёнғинга қарши ускуналарни харид қилиш ва керак тарзда жойлаштириш керак.

9.1.5 Қўриқланадиган зоналарда ишларни бажариш

Бошқариш воситаси

Қўриқланадиган зоналарда ишлаш бўйича жисмоний муҳофаза ва тавсияларни ишлаб чиқиш ва жорий этиш керак

Жорий этиш бўйича қўлланма

Қуйидаги тавсияларни кўриб чиқиш зарур:

a) ахборот хавфсизлиги зонасининг мавжудлиги ва унда ўтказиладиган ишлар тўғрисида фақат ишлаб чиқариш зарурати туфайли буни билиши зарур бўлган шахслар хабардор қилиниши керак;

b) қўриқланадиган зоналарда хавфсизлик ва ёмон ният билан қилинган хатти-ҳаракатлар имкониятларининг олдини олиш нуқтаи назаридан авторизация қилинган ходимнинг назоратисиз ишлашга йўл қўйилмаслиги керак;

c) хавфсизликинг бўш зоналари жисмонан берк бўлиши ва уларнинг ҳолати вақти-вақти билан текширилиб туриши керак;

d) фото-, видео-, аудио- ёки бошқа мобил телефонларнинг камералари каби ёзувчи ускунани махсус рухсатнома олмасдан ишлатишга йўл қўйилмайди.

Қўриқланадиган зоналарда ишлаш бўйича тадбирлар қўриқланадиган зоналарда ишлайдиган ходим, субпудратчи ва бегона ташкилотларнинг фойланувчилари учун бошқариш воситаларини, шунингдек, у ерда бегона ташкилот томонидан бажариладиган фаолиятни ўз ичига олади.

9.1.6 Моддий бойликларни қабул қилиш ва юклаш зоналарини, шунингдек умумий фойдаланиш зоналарини ажратиш

Бошқариш воситаси

Моддий бойликларни қабул қилиш ва юклаш зоналари, шунингдек, хонага кириш мумкин бўлган бошқа жойлар назорат остида бўлиши ва

рухсатсиз фойдаланишга иложи борича йўл қўймаслик учун ахборотга ишлов бериш воситаларидан ажратилган бўлиши керак.

Жорий этиш бўйича қўлланма

Қуйидаги тавсияларни кўриб чиқиш зарур:

a) бинонинг ташқи тарафидан омборхоналарга кириш учун рухсат фақат тегишли ваколатга эга бўлган авторизация қилинган ходимларга берилган бўлиши керак;

b) омборхоналар шундай лойиҳаланган бўлиши керакки, етказиб берувчининг ходимини бинонинг бошқа қисмларига киритмасдан келиб тушаётган моддий бойликларни тушириб олиш мумкин бўлсин;

c) омборхоналарнинг ички эшиги очиқ бўлганда ташқи эшикларининг хавфсизлиги таъминланиши керак;

d) келиб тушаётган моддий бойликлар омборхоналардан фойдаланиш жойларига кўчирилмасдан олдин улар потенциал хавфлар мавжудлигига текширилиши керак (9.2.1d);

e) келиб тушаётган моддий бойликлар активларни бошқариш тартибига мувофиқ рўйхатдан ўтказилиши керак (7.1.1);

f) агар мумкин бўлса, келиб тушаётган ва чиқиб кетаётган юкларни жисмонан ажратиш керак.

9.2 Ускунанинг хавфсизлиги

Мақсад: активларнинг йўқотилиши, шикастланиши, ўғирланиши ёки компрометация қилиниши ва ташкилот узлуксиз иши бузилишининг олдини олиш.

Ускунани хавфсизликнинг бузилиши таҳдидларидан ва атроф-муҳит келтириб чиқарадиган хавфлардан муҳофаза қилиш зарур. Маълумотлардан рухсатсиз фойдаланишларнинг хавфини камайтириш ва уларни йўқотиш ҳамда шикастланишдан муҳофаза қилиш учун ускунанинг (жумладан ташкилотдан ташқарида фойдаланадиганларининг) хавфсизлигини таъминлаш керак. Бунда ускунанинг жойлашиши ва уни кўчириш мумкинлиги билан боғлиқ ўзига хос хусусиятларни эътиборга олиш керак. Муҳитнинг хавфли таъсиридан ёки сақлаб турувчи инфратузилмалар, хусусан электр таъминот тизими ва кабель ажраткичи орқали рухсатсиз фойдаланишдан муҳофаза қилишнинг махсус тадбирлари талаб қилиниши мумкин.

9.2.1 Ускунани жойлаштириш ва муҳофаза қилиш

Бошқариш воситаси

Ускунани шундай жойлаштириш ва муҳофаза қилиш керакки, атроф-муҳит таъсиридан келиб чиқадиган хавфлар ва рухсатсиз фойдаланиш имкони камайсин.

Жорий этиш бўйича қўлланма

Ускунани муҳофаза қилиш учун қуйидаги тавсияларни кўриб чиқиш зарур:

a) ускуна шундай жойлаштирилиши керакки, унинг жойлашган жойларига ортиқча кириш минимумга етказилсин;

b) конфиденциал ахборотга ишлов бериш ва сақлаш воситалари шундай жойлаштирилиши керакки, уларнинг ишлашини рухсатсиз кузатиш хавфи камайсин, шунингдек, рухсатсиз киришнинг олдини олиш учун ахборот тўплагичларни муҳофаза қилиш керак;

c) зарур муҳофазанинг умумий даражасини ошириш учун махсус муҳофазани талаб қиладиган ускунанинг алоҳида элементларини ажратиш зарур;

d) ўғирлик, ёнғин, портлаш, тутунга тўлиш, сув тошиши (сув беришда узилишлар), чанг, тебраниш, кимёвий таъсирлар, электр таъминотда халақитлар, электромагнит нурланиш ва вандализм каби потенциал таҳдидлар ҳавфини минимумга етказиш учун ахборот хавфсизлигини бошқариш воситаларини жорий этиш керак;

e) ахборотга ишлов бериш воситалари яқинида овқатланиш, ичимликлар ичиш ва чекишга тегишли ташкилотнинг ўз сиёсатини белгилаш ва тасдиқлаш зарур;

f) ахборотга ишлов бериш воситаларининг ишлашига ножўя таъсир кўрсатиши мумкин бўлган шароитларни аниқлаш мақсадида атроф-муҳит ҳолатининг мониторингини ўтказиш керак;

g) барча биноларда яшин қайтаргичлардан фойдаланиш, шунингдек, барча кирувчи куч линияларини ва телекоммуникация линияларини яшиндан муҳофаза қилувчи махсус фильтрлар билан жиҳозлаш зарур;

h) ишлаб чиқариш цехларида жойлашган ускуналарнинг махсус муҳофаза қилиш воситалари, масалан, клавиатура учун муҳофазалаш плёнкаси ишлатилиши керак;

i) нурланишнинг қўшимча каналлари бўйлаб ахборотнинг тарқалиш хавфини камайтириш учун конфиденциал ахборотга ишлов бераётган ускунани муҳофаза қилиш керак.

9.2.2 Коммунал ускуна

Бошқариш воситаси

Ускунани электр энергиянинг узатилишидаги ва коммунал ускунадаги авариялар туфайли тўхтаб қолишлар билан боғлиқ бошқа бузилишлардан муҳофаза қилиш зарур.

Жорий этиш бўйича қўлланма

Электр ускуна, сув қувурлари, канализация, иситиш/шамоллатиш ва ҳавони кондициялаш каби барча коммунал ускуналар у таъминлайдиган тизимга мувофиқ бўлиши керак. Коммунал ускунанинг керак тарздаги ишлашини таъминлаш, шунингдек, хавфлар ва тўхтаб қолишларни камайтириш учун уни мунтазам кўздан кечириш ва керак тарзда текшириш керак. Ускунани ишлаб чиқарувчининг тавсияларига мос келадиган электр таъминотининг керак тарзда узатилишини таъминлаш зарур.

Сезгир бизнес жараёнларни сақлаб турувчи ускуна учун ишнинг тўғри тугатилишини ёки қурилмаларнинг узлуксиз ишлашини таъминловчи (Uninterruptable Power Supply, UPS) узлуксиз таъминлаш манбаини ўрнатиш тавсия этилади. Узлуксиз ишни таъминлаш режаларида UPS тўхтаб қолганда қўлланиши керак бўлган хатти-ҳаракатлар кўзда тутилиши керак. Электр таъминоти ишдан узоқ тўхтаб қолганда, агар узлуксиз ишни таъминлашга талаблар бўлса, резерв генератордан фойдаланиш заруратини кўриб чиқиш керак. Генераторнинг ишини таъминлаш учун узоқ муддат давомида ёнилғининг тегишли равишда етказиб берилишини таъминлаш зарур. Тегишли равишда ишлаб туришини таъминлаш учун UPS ускуна ва генераторларни вақти-вақти билан текшириб туриш, шунингдек, уни ишлаб чиқарувчининг тавсияларига мувофиқ текшириш керак. Бундан ташқари, бир неча истеъмол қилиш манбаларидан фойдаланиш, агар объект йирик бўлса - алоҳида кичик станциядан фойдаланиш масаласи кўриб чиқилиши керак.

Электр таъминотнинг аварияга оид узиб улагичларини авария ҳолатида электр таъминотни узиб қўйишни тезлаштириш учун ускуна жойлашган хонанинг қўшимча чиқишлари ёнида жойлаштириш зарур. Асосий электр таъминот тўхтаб қолган ҳолда, авария ҳолатида ёритиш таъминланиши керак.

Ҳавони кондициялаш ва намлаш ускунаси учун, шунингдек, ёнғинни ўчириш тизимлари (агар ишлатилса) учун доимийликни ва сув таъминотининг мувофиқлигини таъминлаш керак. Сув таъминоти тизимининг носоз иши ускунани шикастлаши ёки ёнғин ўчириш тизимининг самарадорлигига қаршилик қилиши мумкин. Агар зарурат бўлса, коммунал ускунанинг носоз ишини аниқлаш учун хабар бериш тизимини баҳолаш ва ўрнатиш керак.

Телекоммуникациялар линияларидан бири бузилганда доимий телефон алоқага эга бўлиш учун телекоммуникациялар ускуналарини коммунал хизматларини етказиб берувчилари билан камида иккита турли маршрут орқали улаш керак. Телефон алоқа фавқулодда вазиятлар бўйича маҳаллий қонунчилик талабларига мос келиши керак.

Бошқалар

Электр таъминотининг узлуксиз электр таъминотини таъминлаш вариантлари сифатида йўқолиб кетишининг олдини олиш учун электр таъминотининг бир нечта линияларидан фойдаланилади.

9.2.3 Кабелларнинг хавфсизлиги

Бошқариш воситаси

Маълумотлар узатиладиган ёки бошқа ахборот хизматлари амалга ошириладиган катта токка мўлжалланган кабеллар ва телекоммуникация кабелларини шикастланишдан ёки ахборотни қўлга туширишдан муҳофаза қилиш керак.

Жорий этиш бўйича қўлланма

Кабелнинг хавфсизлигини таъминлаш учун қуйидаги тавсияларни кўриб чиқиш зарур:

a) кучли токка мўлжалланган кабеллар ва ахборотга ишлов бериш воситаларини боғловчи телекоммуникация линиялари иложи борича ер остида ётқизилган бўлиши ёки адекват муқобил методлар билан муҳофазаланган бўлиши керак;

b) тармоқ кабеллари авторизация қилинмаган уланишлардан ёки шикастланишлардан муҳофазаланган бўлиши керак, масалан, махсус қопламалар ва/ёки ҳамма эркин фойдаланиши мумкин бўлган участкаларни четлаб кабель ётқизиш маршрутини танлаш ёрдамида;

c) халақитлардан мустасно бўлиш учун кучли токка мўлжалланган кабеллар телекоммуникация кабелларидан ажратилган бўлиши керак;

d) кабеллар ва ускуна билан ишлашда нотўғри тармоқ кабелларини тасодифан коммутация қилиш каби хатоларни минимумга келтириш учун аниқ таниладиган маркалашдан фойдаланиш керак;

e) мумкин бўлган хатоларни қисқартириш учун коммутация қилишнинг ҳужжатлаштирилган рўйхатидан фойдаланиш керак;

f) сезгир ёки критик тизимлар учун ахборот хавфсизлигини бошқариш бўйича қўшимча тадбирлар қуйидагиларни ўз ичига олади:

1) зирҳланган қопламалардан фойдаланиш, шунингдек, оралиқ назорат пунктларида ва охирги пунктларда хоналарни беркитиш;

2) кабель ётқизишнинг такрорланадиган маршрутларидан ёки ахборот узатишнинг керак бўлган хавфсизлигини таъминловчи муқобил усулларидан фойдаланиш;

3) оптик-толали алоқа линияларидан фойдаланиш;

4) кабелларни муҳофаза қилиш учун электромагнит экранлашдан фойдаланиш;

5) техник зондлашни инициация қилиш ва кабель тармоғига рухсат берилмаган қурилмаларнинг уланишини физик текшириш;

6) коммутация қилиш панелларидан ва кабель хоналаридан назоратли фойдаланиш.

9.2.4 Ускунага техник хизмат кўрсатиш

Бошқариш воситаси

Ускунанинг доимий ишлаб туришини ва бутлигини таъминлаш учун унга зарур бўлган техник хизмат кўрсатилиши керак.

Жорий этиш бўйича қўлланма

Қуйидаги тавсияларни кўриб чиқиш зарур:

a) ускунага етказиб берувчи томонидан тавсия этиладиган йўриқномаларга ва даврийликка мувофиқ хизмат кўрсатилиши керак;

b) ускунага техник хизмат кўрсатиш ва уни таъмирлаш фақат тегишли ваколатга эга бўлган ходим томонидан амалга оширилиши зарур;

c) барча кўзда тутилган ва/ёки ҳақиқатда бор бўлган носозликлар ҳамда профилактик ва тикловчи техник хизмат кўрсатишнинг барча турлари рўйхатга олиниши керак;

d) ускунага хизмат кўрсатишда, хизмат қаерда кўрсатилиши эътиборга олинган ҳолда, мақбул бошқариш воситаларини қабул қилиш керак: ходим томонидан жойидами ёки ташкилотдан ташқаридами; зарур бўлганда ускунадан конфиденциал ахборотни чиқариб ташлаш, ёхуд хизмат кўрсатадиган ходимни синчиклаб танлаш керак;

e) суғурта қилиш қоидалари томонидан белгиланадиган барча талабларга риоя қилиш керак.

9.2.5 Ташкилот хоналаридан ташқарида ишлатиладиган ускунанинг хавфсизлигини таъминлаш

Бошқариш воситаси

Ускуна ташкилот биносидан ташқарида ишлаганда турли хавфларни эътиборга олган ҳолда, ташкилот ҳудудидан ташқарида турган ускунага нисбатан хавфсизлик чоралари кўрилиши керак.

Жорий этиш бўйича қўлланма

Ускунанинг мансублигидан қатъи назар, ундан ташкилот хоналаридан ташқарида ахборотга ишлов бериш учун фойдаланишга раҳбарият томонидан рухсат берилган бўлиши керак.

Ускунани объектдан ташқарида муҳофаза қилиш бўйича қуйидаги тавсияларни кўриб чиқиш зарур:

a) ташкилот хоналаридан олинган ускуна ва ахборот ташувчиларни умумий фойдаланиш жойларида қаровсиз қолдириш керак эмас. Сафарга чиқиш вақтида портатив компьютерларни қўл юки каби ташиш керак ва имкони борича ундаги маълумотлар эълон қилинмаслиги керак;

b) ишлаб чиқарувчиларнинг ускунани муҳофаза қилиш бўйича йўриқномаларига доимо риоя қилиш зарур, масалан кучли электромагнит майдонларнинг таъсиридан;

c) уйда ишлаганда хавфларнинг аҳамиятини ҳисобга олган ҳолда, ахборот хавфсизлигини бошқариш бўйича тўғри келадиган тадбирларни қўллаш керак, масалан қулфланадиган файл-кабинетлардан фойдаланиш, «тоза стол» сиёсатига амал қилиш ва компьютерлардан фойдаланиш имконини назорат қилиш керак (ISO/IEC 18028 «Тармоқларнинг хавфсизлиги»);

d) ускунани офисдан ташқарида муҳофаза қилиш учун етарли даражада суғурта қилишдан фойдаланиш керак.

Масалан, шикастланиш, ўғирлик ва эшитиб олиш билан боғлиқ хавфсизлик хавфлари сезиларли даражада ускунанинг ташкилотда жойлашишига боғлиқ бўлиши мумкин ва ахборот хавфсизлигини бошқариш бўйича кўпроқ тўғри келадиган тадбирларни аниқлаш ва танлашда ҳисобга олиниши керак.

Бошқалар

Ахборотга ишлов бериш ва уни сақлаш бўйича ускуна шахсий компьютерлар, электрон ён дафтарчалар, мобил телефонларнинг барча турларини, шунингдек, уйда ишлаш учун фойдаланиладиган ёки одатдаги жойлашган жойидан ташқарига транспортда ташиладиган қоғоз ёки бошқа моддий бойликларни ўз ичига олади.

Мобил ускунани муҳофаза қилишнинг бошқа жиҳатлари тўғрисидаги аниқроқ ахборот 11.7.1-бандда келтирилган.

9.2.6 Хавфсиз утилизация қилиш ёки ускунадан такроран фойдаланиш

Бошқариш воситаси

Ҳар қандай сезгир маълумотлар ва лицензион дастурий таъминотни йўқ қилиш ёки хавфсз қайта ёзиш учун утилизация қилишдан аввал барча ахборот ташувчилар (ичига ўрнатилган қаттиқ дисклар)ни барча сезгир маълумотларни йўқ қилиш предметига текшириш керак.

Жорий этиш бўйича қўлланма

Конфиденциал ахборотга эга бўлган хотирловчи қурилмаларни жисмонан бузиш ёки ахборотни йўқ қилиш ва форматлашнинг стандарт функцияларидан фойдаланмасдан хавфсиз тарзда қайта ёзиш зарур.

Бошқалар

Конфиденциал ахборотга эга бўлган шикастланган хотирловчи қурилмалар учун, уларга нисбатан қандай чоралар кўрилиши - йўқ қилиш, қайта тиклаш ёки яроқсиз деб топиш учун хавфларни баҳолаш талаб қилиниши мумкин.

Ахборот пала-партиш утилизация қилинганлиги ва ускунадан қайта фойдаланилганлиги натижасида ошкор этилиши мумкин (10.7.2).

9.2.7 Мол-мулкни олиб чиқиш

Бошқариш воситаси

Ускуна, ахборот ёки дастурий таъминотни ташкилот хоналаридан фақат тегишли рухсатнома бўлганда олиб чиқиш мумкин.

Жорий этиш бўйича қўлланма

Қуйидаги тавсияларни кўриб чиқиш зарур:

a) ускуна, ахборот ёки дастурий таъминотни ташкилот хоналаридан фақат тегишли рухсатнома бўлганда олиб чиқиш мумкин;

b) активларни ташкилот ташқарисига кўчириш учун рухсат бериш ваколатига эга бўлган ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчиларини аниқ тайинлаш керак;

c) ускунани олиб чиқиш учун вақт диапазонини белгилаш, шунингдек, қайтарилаётган ускунанинг мувофиқлиги текширилиши керак;

d) зарурат ва жоиз бўлган жойда, ускунани олиб чиқиш/олиб киришда рўйхатдан ўтказиш, шунингдек, у қайтарилганлиги тўғрисида белги қўйиш керак.

Бошқалар

Рухсат берилмаган ёзув қурилмалари, қуроллар ва шу кабиларни аниқлаш ва уларнинг объект ичига киришининг олдини олиш мақсадида, шунингдек, мол-мулкни рухсатсиз олиб чиқилишини аниқлаш учун танлаб текширувлар ўтказилиши мумкин.

Бундай танлаб ўтказиладиган текширувларни қонун ҳужжатларига ва нормативларга мувофиқ ўтказиш керак. Одамларни танлаб ўтказиладиган текширувлар тўғрисида хабардор қилиш керак, бундай текширувларни фақат юридик ва норматив талабларга мувофиқ рухсат мавжудлигида ўтказиш керак.

10 Маълумотларни узатишни ва операцион процедураларни бошқариш

10.1 Операцион процедуралар ва мажбуриятлар

Мақсад: ахборотга ишлов бериш воситалари керак даражада ва хавфсиз ишлашига ишонч ҳосил қилиш.

Барча ахборотга ишлов бериш воситаларини бошқариш ва уларнинг ишлаши бўйича мажбурият ва процедуралар белгиланган бўлиши керак. Улар тегишли эксплуатацион йўриқномалар ва инцидентларга муносабат билдириш процедураларини ишлаб чиқишни ўз ичига олиши керак.

Пала-партишлик ёки ғараз ният натижасида тизимлардан нотўғри фойдаланишда хавфни минимумга келтириш мақсадида имкони борича ваколатларни бўлишиш принципини амалга ошириш керак.

10.1.1 Операцион процедураларни ҳужжатли расмийлаштириш

Бошқариш воситаси

Операцион процедураларни ҳужжатлаштириш, сақлаб туриш керак ва уларга муҳтож бўлган барча фойдаланувчилар улардан фойдалана оладиган бўлишлари керак.

Жорий этиш бўйича қўлланма

Ишлов бериш тизимларига хизмат кўрсатиш ва ахборот алмашинувига тегишли операцион процедуралар, хусусан компьютер(лар)ни ишга тушириш ва ишини хавфсиз тугатиш процедуралари, резервлаш, ускунага кундалик хизмат кўрсатиш ва таъмирлаш, компьютерли ва коммуникацион ускунали хоналарнинг керак бўлган хавфсизлигини таъминлаш прроцедуралари ҳам ишлаб чиқилган бўлиши керак.

Операцион процедуралар муайян топшириқлар ва масалаларни бажариш бўйича батафсил йўриқномаларни, жумладан қуйидагиларни ўз ичига олиши керак:

а) ахборотга ишлов бериш ва уни бошқариш;

b) резервлаш (10.5);

c) тизимлар ўртасидаги боғлиқликни ўз ичига олган топшириқларни бажариш жадвалига тегишли талабларни белгилаш; илк топшириқни бажаришни бошлаш вақти ва энг охирги топшириқни тугатиш вақти;

d) топшириқни бажариш давомида пайдо бўлиши мумкин бўлган хатоларга ёки бошқа алоҳида вазиятларга, жумладан тизим утилитларидан фойдаланиш учун чеклашларга ишлов бериш (11.5.4);

e) кутилмаган операцион ёки техник муаммолар бўлган ҳолда зарур алоқалар;

f) маълумотларни чиқаришни бошқариш бўйича махсус тадбирлар, масалан босиб чиқарадиган қурилмалар учун махсус қоғоздан ёки, конфиденциал ахборотни чиқариш учун ўзига хос процедуралардан, жумладан топшириқни бажариш жараёнида охирига етказилмаган чиқувчи маълумотларни хавфсиз утилизация қилиш учун процедуралардан фойдаланиш (10.7.2, 10.7.3);

g) тизимни қайта ишга тушириш ва тизим тўхтаб қолган ҳолатларда процедурани қайта тиклаш;

h) баённомалар ахборотларини ва тизим журналларини бошқариш (10.10).

Тизим амаллари бўйича ҳужжатлаштирилган операцион процедуралар расмий ҳужжат сифатида кўриб чиқилиши керак. Уларга киритиладиган ўзгартиришлар раҳбарият томонидан рухсат этилган ва тасдиқланган бўлиши керак. Техник имкониятлар мавжудлигида ахборот тизимларини бир хил процедуралар, асбобсозлик воситалари ва утилитларни қўллаган ҳолда сўзсиз бошқариш керак.

10.1.2 Ўзгаришларни бошқариш

Бошқариш воситаси

Ахборотга ишлов бериш воситалари ва тизимларида конфигурация ўзгаришларини бошқариш керак.

Жорий этиш бўйича қўлланма

Операцион тизимлар ва амалий дастурий таъминот ўзгаришларини жиддий бошқариш керак. Хусусан, қуйидаги пунктларни кўриб чиқиш зарур:

a) катта ўзгаришларни идентификация қилиш ва рўйхатдан ўтказиш;

b) ўзгаришларни режалаштириш ва текшириш;

c) бундай ўзгаришларнинг мумкин бўлган оқибатларини хавфсизликка таъсирини ҳисобга олган ҳолда баҳолаш;

d) таклиф қилинаётган ўзгаришларни тасдиқлашнинг расмий процедураси;

e) барча манфаатдор шахсларни ўзгаришлар тўғрисида батафсил хабардор қилиш;

f) дастурий таъминот муваффақиятсиз ўзгартирилган ва кутилмаган ҳолларда, ахборотга ишлов бериш воситалари ва тизимларининг ишини

тўхтатиб қўйиш ва тиклаш бўйича мажбуриятларни белгилайдиган процедуралар.

Ускуна, дастурий таъминот ёки процедуралардаги барча ўзгаришларнинг керак бўлган бошқарувини таъминлаш мақсадида процедуралар ва раҳбарларнинг расмий жавобгарлиги мавжуд бўлиши керак. Дастурий таъминот ўзгарганда барча зарур ахборот аудитнинг тизим журналида қайд қилиниши ва сақланиши керак.

Бошқалар

Ахборотга ишлов бериш воситалари ва тизимларининг етарли бўлмаган даражаси тизимнинг тўхтаб қолишлари ва хавфсизлик бузилшининг кенг тарқалган сабабларидан ҳисобланади. Айниқса, тизимни ишлаб чиқариш босқичидан иш режимига узатишда операцион муҳитдаги ўзгаришлар, иловаларнинг ишончлилигига таъсир қилиши мумкин (12.5.1).

Эксплуатацион тизимларга киритиладиган ўзгартиришларни фақат бизнеснинг тизимда хавфнинг ошиши каби асосланган сабаблари мавжудлигида киритиш мумкин. Тизимларни операцион тизимларнинг охирги версиялари билан янгилаш доимо бизнес манфаатида бажарилавермайди, чунки, бу ҳозирги кундаги версиядан фойдаланишга қараганда кўпроқ заифликларни ёки нобарқарорликни келтириб чиқариши мумкин. Шунингдек, қўшимча ўқитиш, лицензия учун сарф-харажатлар, сақлаш, сақлаш учун устама харажатлар, хизмат кўрсатиш ва маъмурий бошқаришда, шунингдек, айниқса миграция жараёнида янги аппарат таъминоти керак бўлиб қолиши мумкин.

10.1.3 Мажбуриятлар чегарасини белгилаш

Бошқариш воситаси

Рухсатсиз ёки атайлаб қилинмаган модификацияни ёки ташкилот активларидан мақсадсиз фойдаланиш ва рухсатсиз фойдаланиш имкониятларини камайтириш учун мажбуриятларни ва жавобгарлик соҳаси чегарасини белгилаш керак.

Жорий этиш бўйича қўлланма

Мажбуриятлар чегарасини белгилаш - бу фойдаланувчиларнинг билмасдан ёки ғараз ният билан атайлаб қилган хатти-ҳаракатлари оқибатида тизимлардан штатсиз фойдаланиш хавфини минимумга келтириш усули. Ходим ўзининг якка жавобгарлик соҳасида фош этилмасдан ўз манфаати учун фойдаланиши мумкин бўлмаслик чораларини кўриш зарур. Ҳодисаларни инициация қилиш уни авторизация қилишдан алоҳида бўлиши керак. Бошқариш воситаларини ишлаб чиқишда тил бириктириш хавфи мавжудлигини ҳисобга олиш керак.

Кичик ташкилотлар учун ушбу тадбирларга эришиш қийин, бироқ ушбу принцип имкони борича қўлланиши керак. Мажбуриятларни тақсимлаш қийинлашган ҳолларда фаолият мониторинги, аудит журналларидан фойдаланиш, шунингдек маъмурий назорат чоралари каби ахборот хавфсизлигини бошқариш бўйича бошқа тадбирлардан

фойдаланиш кўриб чиқилиши керак. Шу билан бир вақтда хавфсизлик аудити мустақил функция бўлиб қолиши муҳим.

10.1.4 Ишлаб чиқариш, тестдан ўтказиш ва эксплуатация муҳитларини тақсимлаш

Бошқариш воситаси

Рухсатсиз фойдаланиш ёки операцион тизим ўзгаришининг хавфини камайтириш учун ишлаб чиқариш, тестдан ўтказиш ва эксплуатация муҳитларини тақсимлашда ходимларнинг мажбуриятлари ва жавобгарлиги тақсимлаб берилиши зарур.

Жорий этиш бўйича қўлланма

Эксплуатация қилиш вақтида муаммолар келиб чиқишининг олдини олиш учун эксплуатация қилиш, тестдан ўтказиш ва ишлаб чиқариш муҳитлари ўртасида зарур бўлган тақсимлаш даражасини таъминлаш керак, шунингдек, бошқаришнинг қабул қилса бўладиган воситаларини жорий этиш тавсия этилади.

Қуйидаги пунктларни кўриб чиқиш зарур:

a) дастурий таъминотни ишлаб чиқиш режимидан эксплуатация қилиш режимига ўтказиш қоидаларини аниқлаш ва ҳужжатлаштириш керак;

b) ишлаб чиқиш ва эксплуатация қилишда бўлган дастурий таъминотни турли тизимлар ёки компьютерларда ва турли доменлар ёки каталогларда ишга тушириш керак;

c) компиляторлар, редакторлар ва ишлаб чиқишнинг бошқа инструментал воситалари ёки тизим утилитларидан эҳтиёж бўлмаганда орперацион тизимлардан фойдаланилиши мумкин бўлмаслиги керак;

d) тест тизимли муҳитда иложи борича ишчи тизим муҳитини аниқроқ бошқа тизим муҳитига ўхшатиш керак;

e) фойдаланувчилар эксплуатацион ва тест тизимлари учун турли фойдаланиш профилларини қўллашлари керак; меню хатоларининг хавфини камайтириш учун тегишли танитувчи хабарлар акс эттирилиши керак;

f) ёпиқ маълумотларни тест муҳитига кўчириш керак эмас (12.4.2).

Бошқалар

Ишлаб чиқиш ва тестдан ўтказиш билан боғлиқ фаолият жиддий муаммоларнинг, масалан, файллар ёки тизим муҳитининг номақбул ўзгаришларининг, шунингдек, тизимнинг тўхтаб қолишининг сабаби бўлиши мумкин. Бу ҳолда комплекс равишда натижавий тестдан ўтказишни бажариш ва ишлаб чиқувчилар томонидан рухсатсиз фойдаланишнинг олдини оладиган алоҳида муҳитни иш ҳолатида ушлаб туриш керак.

Ишлаб чиқиш ва тестдан ўтказиш учун жавобгар ходим операцион тизимдан ва у билан боғлиқ бўлган ахборотдан фойдаланиш ҳуқуқига эга бўлса, у рухсат берилмаган яширин кодни жорий қилиш ёки операцион тизимнинг маълумотларини ўзгартириш имконига эга бўлади. Бир қатор

тизимларда қўлланиши мумкин бўлган бу имкониятдан ўз манфаатини кўзлаб, айнан фирибгарлик учун ёки текширилмаган ёки зарар келтирувчи кодни жорий қилиш учун фойдаланиш мумкин. Текширилмаган ёки зарар келтирувчи код тизимнинг ишида жиддий муаммоларнинг сабаби бўлиши мумкин. Ишлаб чиқувчилар ва тестдан ўтказувчи мутахассислар ҳам, шунингдек, операцион тизим ва ахборот хавфсизлиги учун таҳдидлар сабаби бўлиши мумкин.

Агар ишлаб чиқиш ва тестдан ўтказиш бир компьютер муҳитида амалга оширилса, бу дастурий таъминот ва ахбортнинг олдиндан кўзланмаган ўзгаришларининг сабаби бўлиши мумкин. Демак, ишлаб чиқиш, тестдан ўтказиш ва эксплуатация қилиш муҳитларини тақсимлаш фавқулодда ўзгаришлар ёки ишчи дастурий таъминот ва маълумотлардан рухсатсиз фойдаланиш хавфини камайтириш учун мақсадга мувофиқ ҳисобланади (12.4.2).

10.2 Бегона ташкилотлар томонидан хизмат кўрсатилишини бошқариш

Мақсад: бегона ташкилотлар билан хизмат кўрсатиш тўғрисида тузилган контрактлар асосида ахборот хавфсизлиги ва хизмат кўрсатишнинг керакли даражасини жорий этиш ва сақлаб туриш.

Ташкилот контрактларнинг бажарилишини текшириши ва назорат қилиши, бегона ташкилотлар билан келишилган барча талабларнинг бажарилишини таъминлаш учун ўзгаришларни бошқариши керак.

10.2.1 Хизмат кўрсатиш

Бошқариш воситаси

Бегона ташкилот томонидан хавфсизликни бошқариш воситалари, маълум хизматлар ва уларни тақдим этиш даражалари бажарилиши таъминланиши керак.

Жорий этиш бўйича қўлланма

Бегона ташкилот томонидан хизмат кўрсатилишига келишилган хавфсизлик чораларини киритиш, хизматлар ва хизмат кўрсатишни бошқариш масалаларини аниқлаш керак. Ташкилот пудрати тадбирлари ҳолатида барча кўчишни талаб этадиган нарсаларнинг зарур бўлган кўчишларини режалаштириш (ахборот, унга ишлов бериш воситалари ва х.), шунингдек, кўчиш даври давомида хавфсизлик сақланишини таъминлаш керак.

Ташкилот бегона ташкилот хизмат кўрсатиш бўйича етарли қувватларга эга эканлигига ва у хизмат кўрсатишда асосий тўхтаб қолишлар ва авариялларда хизмат кўрсатишнинг келишилган узлуксизлик даражаларини сақлаб туришни таъминлаш режаларини амалга оширишга қодирлигига ишонч ҳосил қилиши керак.

10.2.2 Бегона ташкилотлар хизматларини назорат қилиш ва қайта кўриб чиқиш

Бошқариш воситаси

Бегона ташкилотлар томонидан тақдим этиладиган хизматлар, ҳисоботлар ва ёзувларни мунтазам назорат қилиш ва текшириш керак, шунингдек, мунтазам аудит ўтказиш керак.

Жорий этиш бўйича қўлланма

Бегона ташкилотлар хизматларини назорат қилиш ва текшириш ахборот хавфсизлигига тегишли контрактлар шартларига қатъий риоя қилинишини, шунингдек, ахборот хавфсизлиги инцидентлари ва муаммоларини керак тарзда бошқаришни кафолатлаши керак. Бунга хизмат кўрсатишни бошқаришда бегона ташкилот билан ташкилот ўртасидаги қуйидагилар каби ҳамкорлик масалаларини киритиш керак:

a) контрактларга риоя қилинишини текшириш учун хизмат кўрсатиш унумдорлиги даражасини назорат қилиш;

b) бегона ташкилот томонидан хизмат кўрсатиш бўйича бажарилган ҳисоботларни текшириш, шунингдек, контрактлар талаблари бўйича мунтазам учрашувларни ташкил қилиш;

c) ахборот хавфсизлигининг инцидентлари тўғрисида ахборотни тақдим этиш ва контрактлар талаблари ва бошқа ёрдамчи қўлланмалар ва процедуралар бўйича бегона ташкилот ва ташкилот томонидан ушбу ахборотни назорат қилиш;

d) бегона ташкилот баённомалари ва хавфсизлик воқеалари, эксплуатацион муаммолар, рад этишлар, тақдим этиладиган хизмат кўрсатишга тааллуқли тўхтаб қолишлар ва бузилишларни кузатиб бориш ёзувларини текшириш;

e) ҳар қандай юзага келадиган муаммоларни ҳал қилиш ва бошқариш.

Бегона ташкилот билан ҳамкорлик қилиш бўйича мажбуриятлар хизмат кўрсатишни бошқарадиган муайян шахс ёки шахслар гуруҳига юкланган бўлиши керак. Бундан ташқари, ташкилот, бегона ташкилот контракт талабларига мувофиқлиги ва бажарилишини текшириш бўйича жавобгарни тайинлашига ишонч ҳосил қилиши керак. Контракт талабларининг (6.2.3), хусусан, ахборот хавфсизлиги талабларининг бажарилишини назорат қилиш учун етарли техник кўникмага ва активларнинг етарли сонига эга бўлган ходимни тайинлаши керак. Хизмат кўрсатишда камчиликлар аниқланганда тегишли чоралар кўрилиши керак.

Бегона ташкилот конфиденциал ёки сезгир ахборотдан ва унга ишлов бериш воситаларидан фойдаланганда, улар билан ишлаганда ёки уларни бошқарганда ташкилот барча хавфсизлик жиҳатларини бошқариш ва назорат қилишнинг юқори даражасини сақлаб туриши керак. Ташкилотнинг аниқ белгиланган жараёни, формати ва ташкилот ҳисобдорлигининг структураси ёрдамида ўзгаришларни бошқариш, заифликларни идентификация қилиш ва ахборот хавфсизлиги

инцидентлари тўғрисида ҳисобдорлик/хабар бериш каби хавфсизлик билан боғлиқ хатти-ҳаракатларни назорат қилинишини таъминлаши керак.

Бошқалар

Ташкилот пудрат бўйича ишлаганда субпудратчи томонидан ишлов бериладиган ахборот учун охирги жавобгарлик ўзининг зиммасида қолишини билиши керак.

10.2.3 Бегона ташкилотлар хизматларидаги ўзгаришларни бошқариш

Бошқариш воситаси

Ишга тушган тизимларнинг сезгирлигини ва бизнес-жараёнларни, шунингдек, хавфларнинг кейинги таърифини эътиборга олган ҳолда ахборот хавфсизлиги, процедуралар ва бошқариш воситаларининг мавжуд сиёсатларини қувватлаш ва такомиллаштиришни ҳисобга олиб, хизматларни тақдим этишда ўзгаришларни бошқариш керак.

Жорий этиш бўйича қўлланма

Бегона ташкилотлар хизматларидаги ўзгаришларни бошқариш жараёни қуйидагилар эътиборга олинишини талаб қилади:

a) қуйидагиларни амалга оширувчи, ташкилот томонидан бажариладиган ўзгаришлар:

1) кундалик тақдим этиладиган хизматларни яхшилаш;

2) ҳар қандай янги иловалар ва тизимларни ишлаб чиқиш;

3) ташкилот сиёсати ва процедураларини ўзгартириш ёки янгилаш;

4) ахборот хавфсизлиги инцидентларини ҳал этиш ва хавф-сизликни яхшилаш учун янги воситалар;

b) қуйидагиларни амалга оширувчи бегона ташкилотлар хизматларидаги ўзгаришлар:

1) тармоқлардаги ўзгаришлар ва яхшиланишлар;

2) янги технологиялардан фойдаланиш;

3) янги маҳсулотлар ёки янги версиялар/янгиликнинг реклама қилинишининг қабул қилиниши;

4) янги асбоблар ва ишлаб чиқиш муҳитлари;

5) хизматга оид ускунанинг жисмоний жойлашишидаги ўзгариш;

6) етказиб берувчиларнинг ўзгариши.

10.3 Режалаштириш ва тизимларни қабул қилиш

Мақсад: тизимларнинг ишида тўхтаб қолиш хавфини минимумга келтириш.

Маълумотлардан фойдалана олиш ва тизимлар активларини лозим бўлган юкланишни таъминлаш учун олдиндан режалаштириш ва тайёргарлик кўриш зарур.

Тизимларнинг ортиқча юкланиш хавфини камайтириш учун маълумотлар асосида уларни юклашда бўлғуси эҳтиёжини аниқлаш зарур.

Янги тизимларни эксплуатация қилишга қўйилган талаблар аниқланган, ҳужжатлари расмийлаштирилган ва уларни қабул қилиш ҳамда улардан фойдаланишдан олдин тестдан ўтказилган бўлиши керак.

10.3.1 Унумдорликни бошқариш

Қўллаш воситаси

Ахборотга ишлов бериш тизимларнинг зарур бўлган унумдорлигини таъминлаш учун активлардан фойдаланишни назорат қилиш, уларни тўғрилаш, шунингдек, прогноз асосида уларни юклашда бўлғуси эҳтиёжларни аниқлаш керак.

Жорий этиш бўйича қўлланма

Фаолиятнинг ҳар бир янги ва кундалик тури учун қувватларга қўйиладиган талаблар белгиланиши керак. Зарур бўлган жойларда тизимлардан фойдалана олиш имкониятини ва ишлаш самарадорлигини ошириш учун уларни созлаш ва мониторингини ўтказиш керак. Муаммоларни ўз вақтида аниқлаш учун рўйхатдан ўтказувчи бошқариш воситаларидан фойдаланиш керак. Бўлғуси қувватларга қўйиладиган талабларни ишлаб чиқишда янги функционал ва тизим талабларини, шунингдек, ташкилотда ахборот технологияларини ривожлантиришнинг жорий ва истиқболдаги режаларини эътиборга олиш керак.

Уларни ишга туширишда алоҳида эътиборни катта молиявий харажатлар ва вақт талаб қиладиган активларга қаратиш керак; бинобарин, раҳбарият асосий тизим активларидан фойдаланишни назорат қилиши керак. Раҳбарият бизнес-иловалар ёки ахборот тизимини бошқариш воситаларини қўллаб-қувватлаши учун жуда муҳим бўлган компьютер ресурсларидан фойдаланишда умумий эҳтиёж ва тенденцияларни белгилаши керак.

Раҳбарлар бу ахборотдан тизим хавфсизлиги ёки фойдаланувчилар сервисларига таҳдид солувчи потенциал заиф жойларни идентификация қилиш ва бартараф этиш, шунингдек, ахборот хавфсизлигини таъминлаш бўйича тегишли тадбирларни режалаштириш мақсадида фойдаланишлари керак.

10.3.2 Тизимларни қабул қилиш

Бошқариш воситаси

Тизимларни қабул қилишдан аввал янги ва модернизация қилинган ахборот тизимларини, дастурий таъминот янги версияларининг қабул қилиш мезонлари аниқланиши, шунингдек улар зарур бўлган тестдан ўтказилиши керак.

Жорий этиш бўйича қўлланма

Янги тизимларни қабул қилиш учун талаб ва мезонлар аниқ белгиланган, келишилган, ҳужжатлари расмийлаштирилган ва синалган бўлиши керак. Модернизация қилишнинг янги ахборот тизимлари ва янги

версиялари фақат расмий қабул қилиш тугатилганидан сўнг саноатга оид эксплуатация қилиш учун ўтказилиши керак. Расмий қабул қилишдан олдин қуйидагиларни ҳисобга олиш керак:

a) компьютер қуввати ва унумдорлигига қўйилган талабларнинг бажарилишини баҳолаш;

b) тўхтаб қолиш ва қайта ишга туширишдан сўнг қайта тиклаш процедураларини белгилаш, шунингдек узлуксиз ишни таъминлаш режаларини тузиш;

c) намунавий операцион жараёнларни тайёрлаш ва уларни белгиланган стандартларга мувофиқлигини тестдан ўтказиш;

d) ахборот хавфсизлигини бошқариш воситаларининг зарур бўлган тўпламининг мавжудлиги;

e) процедуралар бўйича самарали қўлланмалар ишлаб чиқиш;

f) 14.1-банд талабларига мувофиқ узлуксиз ишни таъминлаш;

g) янги тизим томонидан мавжуд тизимларга ножўя таъсир йўқлигини мажбурий текшириш, айниқса максимал юкланганда, масалан ойнинг охирида;

h) янги тизим томонидан ташкилотнинг умумий хавфсизлигига кўрсатилаётган таъсирининг таҳлилини ўтказишни назорат қилиш;

i) янги тизимларни эксплуатация қилиш ва улардан фойдаланиш учун ходимларни малакали тайёрлашни ташкил қилиш;

j) фойдаланишнинг оддийлиги, чунки бу ходимнинг меҳнат унумдорлигига таъсир қилади ва инсоний омил хатоларини бартараф қилади.

Янги тизимларни ишлаб чиқишнинг барча босқичларида маслаҳатлашиш учун сақлаб туриш (эксплуатация қилиш) хизматлари ва лойиҳалаштирилаётган тизимнинг самарали эксплуатация қилинишини таъминлаш мақсадида фойдаланувчилар жалб этилиши керак. Бунда қабул қилишнинг барча мезонлари тўлиқ қониқтирилганлигини тасдиқлаш учун тегишли тестлар ўтказилиши керак.

Бошқалар

Хавфсизлик талабларига керакли эътибор қаратилаётганлигини текшириш учун қабул қилиш ўз ичига сертификатлаштириш ва аккредитация қилишнинг расмий жараёнини киритиши мумкин.

10.4 Зарар келтирувчи дастурий таъминотдан ва мобил коддан муҳофаза қилиш

Мақсад: дастурий таъминот ва ахборот массивларининг бутлигини муҳофаза қилишни таъминлаш.

Зарар келтирувчи дастурий таъминот жорий қилинишининг олдини олиш ва аниқлаш учун чоралар кўрилиши зарур.

Дастурий таъминот ва ахборотга ишлов бериш воситалари компьютер вируслари, тармоқ «қуртлари», «троя отлари» ва мантиқий бомбалар каби зарар келтирувчи дастурий таъминот жорий қилиниши учун

жуда таъсирчан. Фойдаланувчилар авторизация қилинмаган ёки зарар келтирувчи дастурий таъминотдан фойдаланишнинг хавфи тўғрисида хабардор бўлишлари керак. Зарурат бўлганда, раҳбарлар зарар келтирувчи дастурий таъминотни аниқлаш ва/ёки киришини олдини олиш учун махсус назорат қилиш воситаларининг жорий қилинишини таъминлашлари керак.

10.4.1 Зарар келтирувчи дастурий таъминотдан муҳофаза қилиш

Бошқариш воситаси

Зарар келтирувчи дастурий таъминотни аниқлаш ва киришнинг олдини олиш мақсадида тегишли муҳофаза қилиш воситаларидан фойдаланиш, шунингдек, фойдаланувчиларнинг тегишли хабардорлигини таъминловчи процедураларни шакллантириш зарур.

Жорий этиш бўйича қўлланма

Зарар келтирувчи дастурий таъминотдан муҳофаза қилиш хавфсизлик талабларини англашга, тизимлардан фойдаланишни бошқаришни назорат қилишнинг тегишли чораларига ва ўзгаришларини лозим даражада бошқаришга асосланиши керак. Қуйидаги тадбирларнинг бажарилишини кўриб чиқиш зарур:

a) рухсат берилмаган дастурий таъминотдан фойдаланишни тақиқлайдиган расмий сиёсатни тасдиқлаш (15.1.2);

b) файллар ва дастурий таъминотни ташқи тармоқлар орқали ёки исталган бошқа ахборот ташувчилари ёрдамида олиш билан боғлиқ хавфлардан муҳофаза қилишнинг расмий сиёсатини тасдиқлаш. Ушбу сиёсатда муҳофаза қилиш чораларини кўриш зарурати тўғрисида кўрсатма бўлиши керак;

c) дастурий таъминот ва таъсирчан бизнес-жараёнларни сақлаб турувчи тизим маълумотларини мунтазам инвентаризация қилиш. Шунингдек, тизимда ҳар қандай авторизация қилинмаган ёки ўзгартирилган файлларнинг пайдо бўлиш сабабларини текшириш бўйича расмийлаштирилган процедура зарур;

d) зарур бўлган ҳолларда олдини олиш чораси ёки эскирган процедура сифатида ишга тушириладиган компьютерлар ва ахборот ташувчиларини аниқлаш ва сканлаш учун вирусга қарши дастурий таъминотни ўрнатиш ва мунтазам янгилаш; ўтказиладиган текширувларга қуйидагиларни киритиш керак:

1) шубҳали ёки авторизация қилинмаган ахборот ташувчиларидаги барча файлларни ёки умумий фойдаланишдаги тармоқлардан олинган файлларни ушбу файллар билан ишлашдан аввал вируслар мавжудлигига текшириш керак;

2) электрон почтанинг ҳар қандай жойланмаларини ва чиқариб олинадиган ахборотни улардан фойдаланишдан олдин зарар келтирувчи дастурий таъминот мавжудлигига текшириш керак. Ушбу текширув турли нуқталарда: масалан, электрон почтада, шахсий компьютерларда ёки ташкилот тармоғига киришда ўтказилиши мумкин;

3) веб-саҳифаларда зарар келтирувчи код мавжудлигини текшириш керак;

e) вируслардан муҳофаза қилиш билан боғлиқ бошқарув процедуралари ва мажбуриятларни, шунингдек, вирус ҳужумларидан сўнг хабардор қилиш ва тиклаш масалаларини аниқлаш, ушбу процедураларни қўллашга ўргатиш (13.1, 13.2);

f) вирус ҳужумларидан сўнг тиклаш борасида узлуксиз ишни таъминлаш бўйича тегишли режаларни, жумладан маълумотлар ва дастурий таъминотни резервлаш ва тиклаш бўйича барча зарур тадбирларни тайёрлаш (14);

g) янги зарар келтирувчи код тўғрисидаги ахборотни тақдим этувчи почта жўнатмалари ва/ёки веб-сайтларни текшириш каби ахборотни мунтазам йиғиш тартибини жорий этиш;

h) зарар келтирувчи дастурий таъминотга тегишли барча ахборотни таҳлил қилиш процедураларини жорий этиш, огоҳлантирувчи хабарларнинг аниқлиги ва ахборот учун берилганлигини таъминлаш. Сохта ва ҳақиқий вирусларнинг фарқини аниқлаш учун профессионал манбалардан, масалан, респектабель журналлар, ишонса бўладиган Интернет-сайтлар ёки вирусга қарши дастурий таъминотни етказиб берувчилардан фойдаланиш керак. Ходимлар сохта вируслар муаммолари ва уларни олганда амалга оширилиши керак бўлган хатти-ҳаракатлар тўғрисида хабардор бўлишлари керак.

Бошқалар

Ахборотга ишлов бериш муҳитида зарар келтирувчи коддан муҳофаза қилувчи, турли ишлаб чиқувчиларнинг икки ва ундан ортиқ дастурий маҳсулотларидан параллел фойдаланиш зарар келтирувчи коддан муҳофаза қилиш самарасини ошириши мумкин.

Тавсифлар файлларининг автоматик янгиланишига эришиш учун зарар келтирувчи коддан муҳофаза қилиш бўйича дастурий таъминот ўрнатилиши, муҳофаза қилишнинг долзарблилигини таъминлаш учун сканловчи модуллар ўрнатилиши мумкин. Бундан ташқари, ушбу дастурий таъминот автоматик текширувларни бажариш учун ҳар бир шахсий компьютерда ўрнатилиши мумкин.

Зарар келтирувчи коддан муҳофаза қилиш бўйича оддий бошқариш воситалари томонидан аниқлаш мумкин бўлмаган зарар келтирувчи коднинг пайдо бўлишидан муҳофаза қилиш учун операцион ва авария процедураларини бажаришда эҳтиёткорликка риоя қилиш керак.

10.4.2 Мобил коддан муҳофаза қилиш

Бошқариш воситаси

Мобил коддан фойдаланиш рухсат этилган жойларда конфигурация мобил коднинг ишини аниқ белгиланган хавфсизлик сиёсатига мувофиқ таъминлаши керак, шунингдек, рухсат этилмаган мобил коднинг бажарилишига йўл қўймаслик керак.

Жорий этиш бўйича қўлланма

Рухсат этилмаган хатти-ҳаракатларни бажарувчи мобил коддан муҳофаза қилиш учун:

a) мобил кодни мантиқий изоляция қилинган муҳитда бажариш;

b) мобил коддан ҳар қандай фойдаланишни блокировкалаш;

c) мобил кодни қабул қилишни блокировкалаш;

d) мобил коднинг бошқарилишини текширишни таъминловчи муайян тизимда фойдалана олиши мумкин бўлган техник воситаларни киритиш;

e) мобил коддан фойдалана оладиган активларни бошқариш;

f) мобил кодни ноёб аутентификация қилиш учун криптографик бошқариш воситаларидан фойдаланиш;

Бошқалар

Мобил код - бир компьютердан бошқасига кўчириладиган, ундан сўнг автоматик равишда ижро этиладиган ва фойдаланувчи билан бирга ҳаракат қилмайдиган ёки кам ҳаракат қиладиган маълум функцияларни бажарадиган дастурий таъминот. Мобил коди оралиқ сервисларнинг маълум сони билан боғлиқ.

Мобил кодда зарар келтирувчи коднинг бўлмаслигини таъминлашдан ташқари, мобил кодни бошқариш рухсатсиз фойдаланишдан ёки тизим, тармоқ ёки амалий активларнинг бузилишидан, шунингдек, ахборот хавфсизлигининг бошқа бузилишларидан мустасно бўлиш учун зарур.

10.5 Резервлаш

Мақсад: ахборот ва ахборотга ишлов бериш воситаларининг бутлигини ва улардан эркин фойдалана олишликни таъминлаш.

Тасдиқланган сиёсатга мувофиқ амалий дастурий таъминотни резервлаш (14.1), маълумотлар нусхасини яратиш ва тестдан ўтказиш, шунингдек, уларни ўз вақтида тиклаш процедуралари мунтазам бажарилиши керак.

10.5.1 Ахборотдан резерв нусха кўчириш

Бошқариш воситаси

Резервлашнинг келишилган сиёсатига мувофиқ конфиденциал ахборот ва дастурий таъминотдан резерв нусха кўчириш мунтазам равишда амалга оширилиши керак.

Жорий этиш бўйича қўлланма

Авариядан ёки ташувчининг тўхтаб қолишидан сўнг конфиденциал ахборот ва дастурий таъминотни кафолатли тиклаш учун резервлашнинг тегишли воситаларини таъминлаш керак.

Ахборотни резервлашнинг қуйидаги масалаларини кўриб чиқиш зарур:

a) резервланадиган ахборотнинг зарур ҳажмини аниқлаш;

b) резерв нусхалар тўғрисидаги ёзувларни аниқ ва тўлиқ бажариш, шунингдек, тиклашнинг ҳужжатлаштирилган тартибига риоя қилиш;

c) резервлашнинг миқдори (масалан тўлиқ ёки дифференциал нусха) ва резервлаш частотаси ташкилот бизнеси талабларини, ишга туширилган ахборотнинг хавфсизлик талабларини, шунингдек, ташкилотнинг узлуксиз фаолиятига нисбатан ахборотнинг сезгирлигини акс эттириши керак;

d) асосий объектдаги ҳар қандай фавқулодда вазиятларда шикастланишнинг олдини олиш учун резерв нусхаларни етарли масофада узоқлаштирилган жойда сақлаш;

e) асосий объектдаги хавфсизлик даржасига мувофиқ жисмоний муҳофаза қилишнинг ва атроф-муҳит таъсиридан муҳофза қилишнинг (9) кафолатланган даражасини таъминлаш. Асосий объектда ускунага нисбатан қўлланадиган тадбирлар резерв пунктга ҳам тааллуқли бўлиши керак;

f) фавқулодда вазият юз берганда резерв ускунанинг ишлашига ишончни таъминлаш учун уни тестдан ўтказиш;

g) тиклаш процедураларининг самарадорлигини ва ишга оид процедураларда тиклаш учун ажратиладиган вақт давомида бажариш имкониятини таъминлаш учун уларни текшириш ва тестдан ўтказиш;

h) конфиденциал ахборотнинг резерв нусхаларини шифрлаш воситалари билан муҳофаза қилиш.

Резерв нусха кўчириш процедуралари узлуксиз ишни таъминлаш режаларининг талабларини қондиришга ишонч ҳосил қилиш учун улар ҳар бир алоҳида тизим учун мунтазам тестдан ўтказилиши керак (14). Критик тизимлар учун резервлаш бўйича тадбирлар барча тизим ахборотини, авария ҳолатида тизимни тўлиқ тиклаш учун зарур иловаларни ва маълумотларни қамраб олиши керак.

Конфиденциал ахборотни сақлаш даврларини белгилаш, шунингдек, узоқ сақланадиган архив нусхаларига қўйиладиган талабларни ҳисобга олиш керак (15.1.3).

Бошқалар

Резервлаш ва тиклаш жараёнини соддалаштириш учун резервлаш бўйича тадбирлар автоматлаштирилган бўлиши мумкин. Бундай автоматлаштирилган ечимларни жорий этилгунча ва жорий этилгандан сўнг вақти-вақти билан керак тарзда тестдан ўтказилиши керак.

10.6 Тармоқ хавфсизлигини бошқариш

Мақсад: тармоқларда ахборот хавфсизлигини ва қўллаб-қувватловчи инфратузилма муҳофазасини таъминлаш.

Ташкилот чегараларидан ташқарида жойлашиши мумкин бўлган тармоқлар хавфсизлигини бошқариш маълумотлар оқимига, қонун ҳужжатларига, мониторингга ва муҳофазага эҳтиёткорлик билан муомала қилишни талаб қилади.

Ахборот хавфсизлигини бошқариш бўйича қўшимча тадбирлар умумий фойдаланиш тармоғи орқали узатиладиган конфиденциал маълумотларни муҳофаза қилиш учун керак бўлиб қолиши мумкин.

10.6.1 Тармоқни бошқариш воситалари

Бошқариш воситаси

Тармоқни таҳдидлардан муҳофаза қилиш учун ва тармоқдан фойдаланадиган тизим ва иловаларнинг, жумладан транзит ахборотнинг хавфсизлигини таъминлаш учун тармоқни адекват бошқариш ва назорат қилиш керак.

Жорий этиш бўйича қўлланма

Тармоқ ресурсларини сақлаб туриш учун жавобгар раҳбарлар тармоқлардаги маълумотлар хавфсизлигини бошқариш воситаларининг жорий қилинишини ва уланган сервисларни рухсатсиз фойдаланишдан муҳофаза қилинишини таъминлашлари керак. Хусусан, қуйидаги чораларни ва ахборот хавфсизлигини бошқариш воситаларини кўриб чиқиш зарур:

a) зарурат бўлганда, тармоқ ресурслари ва компьютерларни эксплуатация қилиш учун жавобгарликни тақсимлаш керак (10.1.3);

b) узоқлаштирилган ускунани, жумладан фойдаланувчиларникида ўрнатилган охирги ускунани бошқариш бўйича мажбурият ва процедуралар белгиланиши керак.

c) агар зарур бўлса, умумий фойдаланиш тармоқлари орқали узатиладиган маълумотларнинг конфиденциаллиги ва бутлигини таъминлаш учун, шунингдек, уланган тизимларни муҳофаза қилиш учун махсус бошқариш воситаларини жорий қилиш керак (11.4, 12.3). Шунингдек, тармоқ серверлари ва ишчи станциялардан фойдаланишни таъминлаш учун махсус бошқариш воситалари керак бўлиб қолиши мумкин;

d) хавфсизликка тааллуқли хатти-ҳаракатларни ёзиш учун воқеаларни рўйхатга олишни ва мониторингини ўтказишни қўллаш керак;

e) бошқариш бўйича хатти-ҳаракатларни бизнесдан сервисга бўлган талаблар билан таққослаш каби ахборотга ишлов бериш инфратузилмасининг хавфсизлигини таъминлашнинг умумий талаблари билан ҳам синчиклаб таққослаб кўриш керак.

Бошқалар

Тармоқ хавфсизлиги тўғрисидаги қўшимча ахборот ISO/IEC 18028 «Ахборот технологиялари - Хавфсизлик методикалари - АТ тармоқларининг хавфсизлиги»да мавжуд.

10.6.2 Тармоқ сервисларининг хавфсизлиги

Бошқариш воситаси

Тармоқ сервислари бўйича барча контрактларга хавфсизлик тавсифлари, хизмат кўрсатиш даражалари ва ушбу сервислар ичкарида ёки ташқаридан тақдим этилишига боғлиқ бўлмаган ҳолда барча тармоқ

сервисларини бошқариш бўйича талаблар белгиланиши ва киритилиши керак.

Жорий этиш бўйича қўлланма

Тармоқ сервислари провайдерининг айтиб ўтилган сервисларни хавсиз бошқариш қобилиятини аниқлаш ва даврий равишда назорат қилиб туриш зарур, шунингдек, аудит ҳуқуқларини келишиш керак.

Хавфсизлик тавсифлари, хизмат кўрсатиш даражалари ва бошқариш талаблари каби алоҳида хизматлар учун зарур, хавфсизлик бўйича тадбирларни белгилаш керак. Ташкилот ушбу чоралар тармоқ сервисларининг провайдери томонидан жорий этилишини таъминлаши керак.

Бошқалар

Тармоқ сервислари уланишларни тақдим этишни, хусусий тармоқ сервисларини, шунингдек, тармоқлараро экранлар ва бузиб киришларни аниқлаш тизимлари каби тармоқ хавфсизлиги бўйича қўшимча сервислар ва бошқарилувчи қурилмалари бўлган тармоқларни ўз ичига олади. Ушбу сервислар учун бошқариб бўлмайдиган ўтказиш полосасига эга оддий фильтрлар каби қўшимча хизматга эга бўлган мураккаб қурилмалардан ҳам фойдаланиш мумкин.

Тармоқ сервисларининг хавфсизлик тавсифлари қуйидагилар ҳисобланади:

a) аутентификация қилиш, шифрлаш ва тармоқ уланишларини бошқариш воситалари каби тармоқ сервисларининг хавфсизлиги учун қўлланадиган технологиялари;

b) хавфсизлик ва тармоқ уланишлари қоидаларига мувофиқ тармоқ сервислари билан хавфсиз уланиш учун талаб қилинадиган техник параметрлар;

c) зарур бўлган жойларда тармоқ сервислари ва иловаларидан фойдаланишни чеклаш учун тармоқ сервисларидан фойдаланиш тартиби.

10.7 Ахборот ташувчиларининг хавфсизлиги

Мақсад: рухсатсиз ошкор қилиш, активларни модификация қилиш, чиқариб юбориш ёки йўқ қилиш ва бизнес жараёнлар узилишининг олдини олиш.

Ҳужжатлар, ахборот ташувчилари (ленталар, дисклар, кассеталар ва ш.к), кириш/чиқиш маълумотлари ва тизим ҳужжатларини шикастланиш, ўғирланиш ва рухсатсиз фойдаланишдан муҳофаза қилишнинг тегишли процедуралари белгиланган бўлиши керак.

10.7.1 Ахборотнинг алмашинадиган ташувчиларини бошқариш

Бошқариш воситаси

Ахборотнинг алмашинадиган ташувчиларини бошқариш тартиби жорий этилиши керак.

Жорий этиш бўйича қўлланма

Ахборотнинг алмашинадиган ташувчиларини бошқариш бўйича қуйидаги тавсияларни кўриб чиқиш зарур:

a) агар кўп маротаба ишлатиладиган ахборот ташувчилар бошқа керак бўлмаса ва улар ташкилот ташқарисига бериладиган бўлса, улар ичидагиларини тиклаш имконисиз йўқ қилиниши керак;

b) ташкилот ташқарисига чиқариладиган ташувчилар тўғрисида доим сақланадиган рўйхатга олиш журналида ёзув ёзилиши зарур, шунингдек, зарур ва мақсадга мувофиқ бўлганда уларни авторизация қилиш қўлланиши керак;

c) барча ахборот ташувчиларини ишлаб чиқарувчиларнинг талабларига мувофиқ ишончли, хавфсиз жойда сақлаш керак;

d) агар ташувчиларда сақланадиган ахборотдан ташувчилар яшаш (ишлаш) муддатига нисбатан (ишлаб чиқарувчиларнинг талабларига мувофиқ) узоқроқ вақт фойдаланиш зарур бўлса, ташувчиларнинг деградация қилиниши туфайли йўқотилишига йўл қўймаслик учун уни бошқа жойда сақлаш керак;

e) маълумотларни йўқотиш имкониятини чеклаш учун алмашинадиган ташувчиларни рўйхатдан ўтказиш масаласини кўриб чиқиш керак;

f) алмашинадиган ташувчиларнинг дисководларини ўрнатишга фақат хизматга оид зарурат бўлганда рухсат бериш керак.

Авторизация қилишнинг барча процедуралари аниқ ҳужжатлаштирилган бўлиши керак.

10.7.2 Ахборот ташувчиларини утилизация қилиш

Бошқариш воситаси

Ахборот ташувчиларидан фойдаланиб бўлгандан сўнг, расмий тартибни қўллаган ҳолда, уларни ишончли ва хавфсиз утилизация қилиш керак.

Жорий этиш бўйича қўлланма

Маълумот ташувчиларини пала-партиш утилизация қилиш натижасида конфиденциал ахборот бегона кишилар қўлига тушиб қолиши мумкин. Бундай хавфни минимумга келтириш учун ахборот ташувчила рини хавфсиз утилизация қилишнинг расмийлаштирилган процедуралари белгиланиши керак. Бунинг учун қуйидаги масалалар кўзда тутилиши зарур:

a) конфиденциал ахборотга эга бўлган ахборот ташувчиларини сақлаш ва ишончли ҳамда хавфсиз (масалан, ёқиш/майдалаш йўли билан) утилизация қилиш керак. Агар ташувчилардан ташкилот доирасида бошқа мақсадлар учун фойдаланиш режалаштирилаётган бўлса, ундаги ахборот йўқ қилиниши керак;

b) хавфсиз утилизация қилиш керак бўлиб қолиши мумкин бўлган ташувчиларни белгилаш тартибини жорий этиш керак;

c) ташувчиларни муҳимлик даражаси бўйича саралашдан кўра барча ахборот ташувчиларига нисбатан хавфсиз утилизация қилиш чоралари кўрилиши осонроқ бўлиши мумкин;

d) кўпгина ташкилотлар қоғоз, ускуна ва ахборот ташувчиларни йиғиш ва утилизация қилиш бўйича хизматларини тақдим этадилар. Тўғри келадиган пудартчини ундаги тажриба ва ахборот хавфсизлиги зарур даражасининг таъминлашини ҳисобга олган ҳолда, синчиклаб танлаш керак;

e) конфиденциал ахборотга эга бўлган ташувчиларини утилизация қилишни имкони борича баённома тузиш учун сақланиши керак бўлган рўйхатга олиш журналида қайд қилиш керак.

Утилизация қилиниши керак бўлган ахборот ташувчилари йиғилиб қолганида «агрегирлаш эффектини» эътиборга олиш керак, яъни йиғилиб қолган махфий бўлмаган ахборотнинг катта ҳажми махфий ахборотнинг кичик ҳажмидан кўпроқ конфиденциал бўлиб қолиши мумкин**.**

Бошқалар

Ташувчилар пала-партиш утилизация қилиниши натижасида ёпиқ ахборот ошкор этилиши мумкин (9.2.6).

10.7.3 Ахборотга ишлов бериш процедуралари

Бошқариш воситаси

Ахборотни рухсатсиз очиш ёки уни нотўғри фойдаланишдан муҳофаза қилинишини таъминлаш мақсадида ахборотга ишлов бериш ва ахборотни сақлаш процедураларини белгилаш зарур

Жорий этиш бўйича қўлланма

Процедуралар ахборотнинг таснифланишини (7.2) ҳисобга олган ҳолда ишлаб чиқилган бўлиши керак.

Қуйидаги масалаларни кўриб чиқиш зарур:*

a) барча ахборот ташувчиларига уларда кўрсатилган таснифлаш даражасига мувофиқ ишлов бериш ва уларни маркалаш;

b) авторизация қилинмаган ходимлар учун фойдаланишни чеклаш;

c) авторизация қилинган маълумот олувчиларининг расмий рўйхатдан ўтказилишини таъминлаш;

d) кирувчи маълумотлар тўлиқлигига, ишлов бериш жараёни лозим даражада якунланаётганлигига ва чиқувчи маълумотлар ишонарли эканлигига ишонч ҳосил қилишни таъминлаш;

e) маълумотлар буферида жойлашган ва конфиденциаллигига мувофиқ чиқарилишини кутаётган ахборотнинг муҳофаза қилинишини таъминлаш;

f) ахборот тушувчиларини ишлаб чиқарувчиларнинг талабларига мувофиқ сақлаш;

g) маълумотларни тарқатишни минимумга келтириш;

h) авторизация қилинган олувчининг эътиборига тақдим этилаётган маълумотларнинг барча нусхаларини аниқ маркалаш;

i) тарқатиш рўйхатлари ва авторизация қилинган олувчиларнинг рўйхатларини мунтазам қайта кўриб чиқиш.

Бошқалар

Ушбу процедуралар ҳужжатлар, ҳисоблаш тизимлари, тармоқлар, шахсий компьютерлар, телекоммуникацияларнинг мобил алоқа воситалари, электрон почта, овозли почта, мультимедиа, почта сервислари/воситалари, факсимиль аппаратлардан фойдаланилганда ва ҳар қандай бошқа ёпиқ тизимлар ва тушувчиларда, масалан, бўш чеклар ва ҳисоблардаги ахборотда қўлланади.

10.7.4 Тизим ҳужжатларининг хавфсизлиги

Бошқариш воситаси

Тизим ҳужжатларини рухсатсиз фойдаланишдан муҳофаза қилиш керак.

Жорий этиш бўйича қўлланма

Тизим ҳужжатларини муҳофаза қилиш учун қуйидаги масалаларни кўриб чиқиш зарур:

a) тизим ҳужжатларини ишончли жойда сақлаш керак;

b) тизим ҳужжатларидан фойдаланиш имконига эга бўлган шахслар рўйхатини минимумга келтириш керак, фойдаланишнинг ўзи эса, бизнес-илова эгаси томонидан авторизация қилинган бўлиши керак;

c) умумий фойдаланиш тармоғи орқали олинадиган/сақланадиган тизим ҳужжатларини тегишлича муҳофаза қилиш керак.

Бошқалар

Тизим ҳужжатлари маълум конфиденциал ахборотни, масалан, бизнес-иловалар ишини, процедураларни, маълумотлар структурасини, авторизация қилиш жараёнларининг таърифларини ўз ичига олиши мумкин.

10.8 Ахборот алмашинуви

Мақсад: ташкилот ичида ва исталган ташқи юридик шахс билан ахборот алмашинувида ахборот хавфсизлигини ва дастурий таъминотни сақлаш.

Ташкилотлар ўртасида ахборот ва дастурий таъминот билан алмашинувни алмашинув бўйича битимларга мувофиқ олиб бориладиган алмашинувнинг расмий сиёсатида, шунингдек, амалдаги қонун ҳужжатларига мувофиқ асослаш керак (15).

Ахборот ва тушувчиларни транспортда ташиш ва узатишда муҳофаза қилиш бўйича процедура ва тадбирлар белгиланиши зарур.

10.8.1 Ахборот алмашинувининг сиёсати ва процедуралари

Бошқариш воситаси

Ахборот алмашинувини телекоммуникация воситаларининг барча турлари ёрдамида муҳофаза қилиш учун алмашинувни бошқаришнинг

расмий сиёсатини, тартибини ва бошқариш воситасини ишлаб чиқиш керак.

Жорий этиш бўйича қўлланма

Ахборот алмашинуви учун телекоммуникацияларнинг электрон воситаларидан фойдаланишда риоя қилиниши керак бўлган тартиб ва воситалар ўз ичига қуйидаги масалаларни олиши керак:

a) ахборотни қўлга тушириш, ундан нусха кўчириш, ўзгартириш, нотўғри маршрутлаш ва йўқ қилишдан муҳофаза қилишнинг ишлаб чиқилган тартиби;

b) аниқлаш ва телекоммуникациялар ёрдамида узатилиши мумкин бўлган зарар келтирувчи дастурий таъминотдан муҳофаза қилиш тартиби (10.4.1);

c) илова шаклида узатиладиган конфиденциал электрон ахборотни муҳофаза қилиш тартиби;

d) телекоммуникацияларнинг электрон воситаларидан йўл қўйилган фойдаланишни таърифловчи сиёсат ёки қўлланма (7.1.3);

e) симсиз телекоммуникациялардан амалдаги хавфларни эътиборга олиб фойдаланиш тартиби;

f) ходим, субпудратчи ва бошқа фойдаланувчиларнинг хатти-ҳаракатлари ташкилотнинг обрўсини тўкмаслиги керак, масалан, ёлғонни тарқатиш, талаб қилиш, ўзини бошқа шахс сифатида кўрсатиш, хатларни кетма-кет йўллаш, рухсатсиз харид қилиш ва ҳ. йўли билан;

g) криптографик методлардан фойдаланиш, масалан, конфиденциалликни, бутликни ва ахборотнинг ҳақиқийлигини муҳофаза қилиш учун (12.3);

h) барча хизматга оид ёзишмани, жумладан амалдаги барча қонун ҳужжатлари ва нормаларга мувофиқ хабарларни сақлаш ва утилизация қилиш бўйича қўлланма;

i) конфиденциал ва сезгир ахборотни босиб чиқарадиган қурилмаларда, масалан нусха кўчириш қурилмалари, принтерлар ва факсимиль аппаратларда қолдирмаслик керак, чунки улардан авторизация қилинмаган ходим фойдаланиши мумкин;

j) телекоммуникациялар воситаларини қайта йўналтириш, масалан, электрон почтани ташқи почта манзилларга автоматик равишда қайта йўналтириш билан боғлиқ бошқариш ва чеклаш воситалари;

k) конфиденциал ахборотнинг ошкор қилинишига йўл қўймаслик, масалан, телефон музокараларини олиб бориш вақтида ахборотни эшитиб олиш ва қўлга туширишдан мустасно бўлиш учун ходимга тегишли эҳтиёт чораларини кўриш зарурати тўғрисида эслатиш:

1) бевосита яқин турган шахслар томонидан, айниқса мобил телефонлардан фойдаланилганда;

2) телефон аппарати, телефон линиясига жисмонан кириш йўли билан ёки шунга ўхшаш мобил телефонларни қўллаганда сканер қилувчи қабул қилгичлар ёрдамида телефон сўзлашувларини эшитиб олиш;

3) адресат томонидаги бегона шахслар томонидан;

l) автожавоб бергичларда хабар қолдиришни ман этиш, чунки бу хабарлар авторизация қилинмаган шахслар томонидан қайта эшиттирилиши, умумий фойдаланиш тизимларида сақланиши ёки нотўғри номер териш натижасида нотўғри сақланиши мумкин;

m) факсимиль аппаратлардан фойдаланишга хос бўлган хавфларнинг мумкинлиги тўғрисида ходимларга эслатиб қўйиш, айнан:

1) хабарларни қидириш учун ичига ўрнатилган хотирадан рухсатсиз фойдаланиш;

2) хабарларни белгиланган рақамлар бўйича узатиш мақсадида атайлаб ёки тасодифан қайта дастурлаш;

3) номерни нотўғри териш ёки нотўғри сақланган номердан фойдаланиш натижасида ҳужжат ва хабарларни нотўғри номер бўйича юбориш;

n) рухсатсиз фойдаланиш учун шахсий маълумотларни тўплашнинг олдини олиш мақсадида ходим тўғрисидаги, электрон почта манзиллари ва бошқалар каби маълумотларни дастурий таъминотга киритмаслик кераклиги тўғрисида эслатиш;

o) замонавий факсимиль аппаратлар ва фото нусха кўчирадиган қурилмаларда саҳифалар учун кэш-хотира борлиги, қоғоз узатилиши тўхтаб қолган ҳолда ёки узатишда хато бўлганида улар хато йўқолиши билан босиб чиқариладиган саҳифаларни сақлашларини ходимга эслатиш.

Бундан ташқари, конфиденциал суҳбатни жамоат жойларида, очиқ офисларда ва деворлари юпқа бўлган суҳбат олиб бориладиган хоналарда олиб бормаслик керак.

Ахборот алмашинуви воситалари юридик талабларга жавоб бериши керак (15).

Бошқалар

Ахборот алмашинуви телекоммуникацияларнинг кўпгина хилма-хил турлари, жумладан электрон почта, овозли алоқа, факсимиль ва видеоалоқа ёрдамида амалга оширилиши мумкин.

Дастурий таъминот алмашинуви турли ташувчилар, жумладан, интернет тармоғидан юкланиш ва етказиб берувчилардан дастурий маҳсулотларни сотиб олиш ёрдамида амалга оширилиши мумкин.

Маълумотларнинг электрон алмашинуви, электрон савдо ва электрон коммуникациялар билан боғлиқ бўлган хизматга оид, дастлабки юридик шартларни ва хавфсизликнинг дастлабки шартларини, шунингдек, бошқариш воситаларига бўлган талабларни кўриб чиқиш керак.

Ахборот алмашинувининг воситаларидан фойдаланиш сиёсати ва процедураларини билмаслик, масалан, жамоат жойида мобил телефонга билдирмай қулоқ солиш, электрон почта хабарларини нотўғри қайта йўналтириш, автожавоб бергичларга билдирмай қулоқ солиш, овозли почтадан фойдаланганда рухсатсиз кириш ёки факсларни тасодифан хато рақамларга жўнатиш туфайли ахборот компрометация қилиниши мумкин.

Тўхтаб қолиш, ўта юклаш ёки телекоммуникациялар воситаларининг иши тўхтаб қолишида бизнес операциялар тўхтаб қолиши

ва ахборот компрометация қилиниши мумкин (10.3, 14). Ахборот, шунингдек, авторизация қилинмаган фойдаланувчилар фойдаланганда ҳам компрометация қилиниши мумкин (11).

10.8.2 Алмашинув бўйича битим

Бошқариш воситаси

Телекоммуникациялар воситаларининг барча турлари ёрдамида ахборот ва дастурий таъминот алмашинуви учун алмашинувни бошқаришнинг расмий сиёсатини, тартибини ва воситаларини ишлаб чиқиш керак.

Жорий этиш бўйича қўлланма

Алмашинув бўйича контрактларда хавфсизликнинг қуйидаги шартларини кўриб чиқиш керак:

a) раҳбариятнинг ахборотни бошқариш ва узатиш, жўнатиш ва олиш тўғрисида хабардор қилиш бўйича мажбуриятлари;

b) жўнатувчини ахборотни узатиш, жўнатиш ва олиш тўғрисида хабардор қилиш учун процедуралар;

c) кузатиш ва апелляциялаш мумкинлигини таъминлаш тартиби;

d) маълумотлар пакетини шакллантириш ва узатиш бўйича минимал техник талаблар;

e) шартли равишда депозитга қўйиш бўйича контрактлар;

f) курьерларга қўйилган талаблар;

g) ахборот хавфсизлигининг маълумотларни йўқотиш каби инцидентлари ҳолатида жавобгарлик ва мажбуриятлар;

h) конфиденциал ёки сезгир ахборот учун ушбу маркалашнинг маъноси дарҳол тушуниладиган ва ахборот тегишлича муҳофазаланган бўлишига ишонч ҳосил қиладиган маркалашнинг келишилган тизимидан фойдаланиш;

i) ахборот ва дастурий таъминотнинг эгаларини, шунингдек дастурий таъминот ва ҳоказоларга муаллифлик ҳуқуқини, жумладан маълумотларни муҳофаза қилиш бўйича мажбуриятларни аниқлаш (15.1.2, 15.1.4);

j) ахборот ва дастурий таъминотни ёзиш ва ўқиб солиштиришга тегишли техник талаблар;

k) конфиденциал маълумотларни муҳофаза қилиш учун керак бўлиб қолиши мумкин бўлган ҳар қандай махсус воситалар, масалан, криптографик калитлар (12.3).

Ахборотни муҳофаза қилиш ва жисмоний ташувчиларни транспортда ташиш бўйича сиёсат, процедуралар ва стандартларни белгилаш ва қўллаб-қувватлаш керак (10.8.3), юқорида эсга олинган алмашинув бўйича контрактларда ҳам уларга ҳаволалар қилиниши керак.

Бундай битимларда хавфсизлик талаблари алмашинув предмети бўлган ахборотнинг конфиденциаллик даражасини ҳисобга олиши керак.

Бошқалар

Битимлар электрон ёки қўлланмалар қўринишида бўлиши, шунингдек, расмий битимлар ёки меҳнат шартномаси шартларининг шаклларини қабул қилиши мумкин. Конфиденциал ахборотнинг алмашинуви учун муайян механизмлардан фойдаланишни барча ташкилотлар билан тузилган битимларнинг барча турларида келишиш керак.

10.8.3 Транспортда ташишда ахборот ташувчиларининг хавфсизлиги

Бошқариш воситаси

Ахборотга эга бўлган ташувчиларни рухсатсиз фойдаланишдан, ҳуқуқсиз ишлатишдан ва ташкилотнинг жисмоний чегараларидан ташқарида транспортда ташиш вақтида шикастланишдан муҳофаза қилиш керак.

Жорий этиш бўйича қўлланма

Ташкилотлар ўртасида транспортда ташиладиган ахборот ташувчиларини муҳофаза қилиш учун қуйидаги тавсиялар кўриб чиқилиши керак:

a) ишонарли ташувчилар ёки курьерлардан фойдаланиш керак;

b) ваколатли курьерларнинг рўйхатини раҳбарият билан келишиш зарур;

c) курьерларни идентификаци қилишни текшириш тартибини ишлаб чиқиш керак;

d) ўров ахборот ташувчиларини транспортда ташишда мумкин бўлган ҳар қандай жисмоний шикастланишдан муҳофаза қилиш учун етарли бўлиши керак ва ишлаб чиқарувчиларнинг талабларига мос келиши керак (мисол учун дастурий таъминотнинг). Ташувчиларнинг тиклаш самарадорлигини пасайтириши мумкин бўлган юқори ҳароратнинг таъсири, намлик ёки электромагнит майдон каби муҳитнинг ҳар қандай омиллари таъсиридан муҳофаза қилиш зарур.

e) конфиденциал ахборотни рухсатсиз очиш ёки модификация қилишдан муҳофаза қилиш учун зарур бўлганда, махсус воситалар қўлланиши керак. Масалан:

1) қулфланадиган контейнерлардан фойдаланиш;

2) шахсан элтиб бериш;

3) билинтирмасдан бузиш мумкин бўлмаган (очиш учун ҳар қандай уриниш билинадиган) ўровдан фойдаланиш;

4) истисно ҳолларда, жўнатмани бир неча қисмларга бўлиш ва турли маршрутлар билан жўнатиш.

Бошқалар

Ахборот рухсатсиз фойдаланиш, нотўғри ишлатиш ёки транспортда жисмонан ташиш вақтида бузилиши оқибатида бузилиши ёки компрометация қилиниши мумкин, масалан, ахборот ташувчиларни почта ёки курьер орқали жўнатишда ахборот бузилиши мумкин.

10.8.4 Хабарлар билан электрон алмашинув

Бошқариш воситаси

Электрон алмашинувда ишлатиладиган ахборотни лозим даражада муҳофаза қилиш керак.

Жорий этиш бўйича қўлланма

Электрон алмашинуви хавфсизлиги масалалари қуйидагиларни ўз ичига олиши керак:

a) хабарларни рухсатсиз фойдаланишдан, модификация қилиш ёки хизмат кўрсатишда бош тортишдан муҳофаза қилиш;

b) хабарларни тўғри адресация қилиш ва транспортда ташиш кафолатлари;

c) хизмат кўрсатишнинг умумий ишончлилиги ва қулайлиги;

d) юридик масалалар, масалан, электрон рақамли имзоларга қўйилган талаблар;

e) бир лаҳзали хабарлар билан алмашинув ёки файллардан биргаликда фойдаланиш каби ҳамма эркин фойдалана оладиган ташқи сервислардан фойдаланиш учун рухсат олиш;

f) умумий фойдаланиш тармоқларидан фойдаланишни бошқаришда аутентификация қилишнинг ишончлироқ методлари.

Бошқалар

Хабарлар билан электрон алмашинуви, масалан, электрон почта, маълумотлар билан электрон алмашинуви (Eltctronic Exhanje Data EDI) ва бир лаҳзалик хабарлар билан алмашинув хизматга оид коммуникацияларда муҳим ўрин тутмоқда. Хабарлар билан электрон алмашинувининг хавфлари қоғозли иш юритишга асосланган коммуникация хавф-ларидан фарқ қилади.

10.8.5 Бизнес учун ахборот тизимлари

Бошқариш воситаси

Бизнес учун ахборот тизимларининг ўзаро алоқаларига тегишли ахборотни муҳофаза қилиш сиёсати ва тартибини ишлаб чиқиш ва жорий қилиш керак.

Жорий этиш бўйича қўлланма

Ушбу тизимларнинг ўзаро алоқалари бўйича бизнес хавфсизлиги ва шартлари масалалари қуйидагиларни ўз ичига олиши керак:

a) ахборотлари ташкилотнинг турли бўлинмалари томонидан фойдаланиладиган маъмурий ва ҳисобга оид тизимлардаги таниқли заифликлар;

b) бизнес-телекоммуникациялар тизимларидаги ахборотнинг заифлиги, масалан, телефон қўнғироқлари ёки конференцияларни ёзиб олиш, қўнғироқларнинг конфиденциаллиги, факсларни сақлаш, почтани очиш ва тақсимлаш;

c) ахборотдан биргаликда фойдаланиш сиёсати ва қабул қилса бўладиган бошқарув воситалари;

d) агар тизим муҳофаза қилишнинг керакли даражасини таъминламаса, бизнеснинг конфиденциал ахборотидан ва грифи бор ҳужжатлардан фойдаланишни ман этиш (7.2);

e) муайян шахсларга, масалан, ёпиқ лойиҳаларда иш олиб бораётган ходимларга тегишли кундаликларнинг ахборотидан фойдаланишни чеклаш;

f) тизимдан фойдаланиш рухсат этилган ходимлар, субпудратчилар ёки хизматга оид шериклар тоифалари, шунингдек, ундан фойдалана олиш мумкин бўлган жойлар (6.2, 6.3);

g) фойдаланувчиларнинг маълум тоифалари учун танланган воситалардан фойдаланишни чеклаш;

h) фойдаланувчилар мақомини идентификация қилиш, масалан, ташкилот хизматчилари ёки субпудратчилар бошқа фойдаланувчилар учун маълумотномаларда;

i) тизимда сақланадиган ахборотни сақлаш ва резервлаш (10.5.1);

j) авария режимига ўтиш бўйича талаблар ва чоралар (14).

Бошқалар

Офис ахборот тизимлари - бу ҳужжатлар, компьютерлар, мобил ҳисоблашлар, мобил алоқалар, почталар, овозли почта, мультимедиа, почта хизматлари/воситалари ва факс-аппаратларни қўшиб фойдаланадиган хизматга оид ахборотни тезроқ тарқатиш ва бирга фойдаланиш имкониятлари.

10.9 Электрон савдо хизматлари

Мақсад: электрон савдо хизматларининг хавфсизлигини ва улардан хавфсиз фойдаланишни таъминлаш.

Хавфсизликнинг электрон савдо билан боғлиқ хавфсизлик шартларини, жумладан он-лайн режимидаги битимларни ва бошқариш воситаларига қўйилган талабларни кўриб чиқиш керак. Ҳамма эркин фойдаланиши мумкин бўлган электрон тизимлар ёрдамида нашр этилган ахборотнинг бутлиги ва ундан фойдалана олиш мумкинлиги масалаларини кўриб чиқиш зарур.

10.9.1 Электрон савдо

Бошқариш воситаси

Умумий фойдаланиш тармоқлари орқали узатиладиган, электрон почтада ишга туширилган, ахборотни фирибгарликдан, контрактлар бўйича баҳслардан, шунингдек, рухсатсиз ошкор қилиш ва ўзгартиришлардан муҳофаза қилиш керак.

Жорий этиш бўйича қўлланма

Электрон савдо хавфсизлиги масалалари қуйидагиларни ўз ичига олиши керак:

a) бошқа томонни идентификация қилиш учун, масалан, аутентификация қилиш йўли билан ҳар бир томон талаб қиладиган ишонч даражаси;

b) нархларни ким белгилаши, асосий савдо ҳужжатларини ким чиқариши ёки ким имзолаши мумкинлиги билан боғлиқ рухсат бериш жараёнлари;

c) ўзининг ваколатлари тўғрисида савдо бўйича шерикларнинг тўлиқ хабардорлигини таъминлаш;

d) конфиденциаллик, бутлик талабларини, асосий ҳужжатларни жўнатиш ва олиш исботларини аниқлаш ва қониқтириш, шунингдек, мажбуриятлардан, масалан, тендерлар ва контрактлардан бош тортиш мукин бўлмаслигини таъминлаш;

e) реклама қилинаётган прейскурантларнинг бутлигига талаб қилинган ишонч даражаси;

f) ҳар қандай ёпиқ маълумотлар ёки ахборотнинг конфиденциаллиги;

g) буюртма, тўлов, элтиб бериш ва олганлигини тасдиқлаш манзилининг батафсиллиги бўйича ахборот ҳар қандай транзакцияларининг конфиденциаллиги ва бутлиги;

h) мижоз томонидан тақдим этилган тўлов бўйича тегишли ахборотни текшириш даражаси;

i) фирибгарликка қарши чоралар кўриш учун тўловларни ташкил қилишнинг мақбулроқ шаклини танлаш;

j) буюртма маълумотларининг конфиденциаллиги ва бутлигини таъминлаш учун талаб қилинадиган муҳофаза қилиш даражаси;

k) йўқотишлар ва транзакция ахбороти такрорланишининг олдини олиш;

l) ҳар қандай фирибгарлик транзакциялари билан боғлиқ жавобгарлик;

m) суғурта қилиш талаблари.

Юқорида эслатиб ўтилган масалаларнинг кўпи юридик талабларга мувофиқлигини эътиборга олиб, бошқаришнинг криптографик воситаларини (12.3) қўллаш билан ҳал қилиниши мумкин (15.1, 15.1.6).

Савдо соҳасидаги шериклар ўртасида электрон савдони ташкил қилишни икки томонга келишилган савдо шартларини, жумладан рухсат бериш бўйича тафсилотларни юклайдиган, ҳужжатлаштирилган контрактлар билан олиб бориш керак (10.9.1b). Шунингдек, ахборот хизматлари ва хизматлар провайдерлари билан бошқа контрактлар тузиш зарур бўлиб қолиши мумкин.

Савдонинг ҳамма эркин фойдаланиши мумкин бўлган тизимлари ўз мижозларини бизнес шартлар билан таништиришлари керак.

Электрон савдо учун фойдаланиладиган сервер(лар) таҳдидларига бардошлиликни, шунингдек, электрон савдо хизматларини тақдим этиш учун зарур бўлган ҳар қандай тармоқ алоқалари хавфсизлигининг дастлабки шартларини кўриб чиқиш керак (11.4.6).

Бошқалар

Электрон савдо фирибгарлик, контракт бўйича баҳслар, шунингдек, ахборотнинг ошкор қилиниши ёки модификация қилинишига олиб келиши мумкин бўлган кўпгина тармоқ таҳдидларига нисбатан таъсирчан.

Электрон савдодаги хавфларни камайтириш учун аутентификация қилишнинг хавфсиз методларидан фойдаланиш мумкин, масалан, очиқ калитлар инфратузилмаси ва электрон рақамли имзолар ёрдамида (12.3). Бундай хизматларга зарурат бўлган жойларда учинчи ишончли шахслардан фойдаланса бўлади.

10.9.2 Реал вақт режимидаги транзакциялар

Бошқариш воситаси

Хабарларни бутлигини бузиш, хато маршрутлаштириш, рухсатсиз ўзгартириш, ошкор қилиш, такрорлаш ёки хабарларни қайта жўнатишнинг олдини олиш учун реал вақт режимидаги транзакцияларда амалда бўлган ахборотни муҳофаза қилиш керак

Жорий этиш бўйича қўлланма

Он-лайн контрактлари хавфсизлигининг масалалари қуйидагиларни ўз ичига олиши керак:

a) транзакцияда жалб этилган ҳар бир томоннинг электрон рақамли имзоларидан фойдаланиш;

b) транзакциянинг барча жиҳатлари, яъни, таъминот;

1) барча томонлар фойдаланиш ваколатларининг ҳақиқийлиги ва тасдиқлари;

2) транзакциянинг конфиденциаллиги;

3) барча жалб этилган томонларнинг конфиденциаллиги;

c) барча жалб этилган томонлар ўртасидаги телекоммуникациялар маршрутини шифрлаш;

d) барча жалб этилган томонлар ўртасидаги телекоммуникациялар баённомаларини муҳофаза қилиш;

e) ҳар қандай умумфойдаланиш шароитидан ташқари транзакциялар бўйича ахборот тўпловчиларнинг жойлашиш тартибини таъминлаш, масалан, ташкилотнинг Интернет тармоғидаги ахборот тўплагич платформасида, Интернет тармоғидан бевосита фойдаланиш мумкин бўлган ташувчида сақлашни ман этиш;

f) агар ишончли тасдиқловчи марказдан (масалан, электрон рақамли имзоларни ва/ёки рақамли гувоҳномаларни нашр қилиш ва қўллаб-қувватлаш учун) фойдаланилса, хавфсизлик комплекс ҳисобланади ва ушбу имзо/гувоҳномаларни бошқариш жараёнининг бутун цикли давомида қўлланади.

Бошқалар

Бошқариш воситаларини қўллаш даражаси реал вақт режимидаги транзакциянинг тури билан боғлиқ хавф даражаси билан таққосланиши керак.

Транзакцияларда транзакция яратилган, ишлов берилган, тугатилган ва/ёки сақланган ўша юрисдикция қонунлари, қоидалари ва йўриқномаларининг бажарилиши талаб қилиниши мумкин.

Он-лайн режимида бажарилиши мумкин бўлган транзакцияларнинг кўп турлари мавжуд, масалан шартномавий, молиявий ва ш.к.

10.9.3 Ҳамма фойдаланиши мумкин бўлган ахборот

Бошқариш воситаси

Рухсатсиз модификация қилишнинг олдини олиш учун фойдаланиш умумий фойдаланиш тизимларидан тақдим этилган ахборотнинг бутлигини муҳофаза қилиш керак.

Жорий этиш бўйича қўлланма

Фойдаланиш умумий фойдаланиш тизимлари орқали амалга ошириладиган дастурий таъминот, маълумотлар ва бутлигининг юқори даражасини талаб қиладиган бошқа ахборотни адекват усуллар билан, масалан электрон рақамли имзо ёрдамида муҳофаза қилиш керак (12.3). Ахборотдан фойдаланиш тақдим этилишидан олдин умумий фойдаланиш тизимини заифликлар ва бузилишлар мавжудлигига текшириш керак.

Ахборотдан ҳамма эркин фойдалана оладиган бўлишидан олдин тасдиқлашнинг расмий жараёни бажарилиши керак. Бундан ташқари тизимга ташқаридан барча киришларни текшириш ва тасдиқлаш керак:

Ахборотни электрон эълон қилиш, интерактив алоқа ва ахборотни бевосита киритиш имконини берувчи тизимлар қуйидагиларни амалга ошириш учун керакли назорат остида бўлиши керак:

a) олинган ахборот маълумотларни муҳофаза қилиш соҳасида қонун ҳужжатларига мувофиқ бўлиши (15.1.4);

b) электрон кўринишда эълон қилинган тизимга киритилган ахборотга ўз вақтида, тўлиқ ва аниқ ишлов берилиши;

c) конфиденциал ахборот уни йиғиш ва сақлаш жараёнида муҳофаза қилинган бўлиши;

d) электрон кўринишда эълон қилинган тизимдан фойдаланиш у боғлиқ бўлган тизимлардан рухсатсиз фойдаланиш имконини мустасно қилган бўлар эди.

Бошқалар

Умумий фойдаланиш тизимининг ахборотини, масалан Интернет тармоғи орқали фойдаланиш мумкин бўлган Web-сайтдаги ахборотни ушбу тизим юрисдикцияси остида бўлган ёки савдо амалга ошириладиган мамлакатнинг қонун ҳужжатлари ва норматив ҳужжатларига мувофиқлаштириш талаб этилиши мумкин. Нашр этилган ахборотни рухсатсиз модификация қилиш ташкилот обрўсига зарар етказиши мумкин.

10.10 Мониторинг

Мақсад: ахборотга ишлов беришда рухсатсиз хатти-ҳаракатларни аниқлаш.

Тизимларни кузатиш мумкинлигини ва ахборот хавфсизлиги воқеаларини рўйхатга олиш керак. Ахборот тизимларининг муаммоларини идентификация қилишни таъминлаш учун тўхтаб қолишлар ва операцияларни рўйхатга олиш журнали юритилиши керак.

Ташкилот воқеаларни кузатиш мумкинлиги ва воқеаларни рўйхатга олиш бўйича хатти-ҳаракатларга қўлланадиган барча тегишли юридик талабларга риоя қилиши керак.

Тизим мониторинги ахборот хавфсизлигини таъминлаш ва фойдаланишни бошқариш сиёсати моделига мувофиқлигини тасдиқлаш бўйича бажариладиган тадбирларнинг самаралилигини текширишга имкон беради.

10.10.1 Аудит журналларини юритиш

Бошқариш воситаси

Ахборот хавфсизлиги инцидентлари, воқеаларини ёзиш учун аудит журналини юритиш ва уларни маълум вақт мобайнида сақлаш керак. Бу журналлар инцидентларнинг кейинги текширувларини ва фойдаланишни бошқариш мониторингини ўтказишда зарур бўлади.

Жорий этиш бўйича қўлланма

Аудит журналлари зарур бўлганда қуйидагиларни ўз ичига олиши керак:

a) фойдаланувчиларнинг идентификаторларини;

b) асосий воқеаларнинг санаси, вақти ва батафсил тафсилотларини, масалан, фойдаланувчиларнинг кириши ва чиқиши;

c) терминал идентификатори ёки мумкин бўлса, унинг жойлашган жойи;

d) тизимдан фойдаланишнинг муваффақиятли ва рад этилган уринишларининг ёзувлари;

e) маълумотлар ва бошқа активлардан фойдаланишнинг муваффақиятли ва рад этилган уринишларининг ёзувлари;

f) тизим конфигурациясини ўзгартириш;

g) имтиёзлардан фойдаланиш;

h) тизим утилитлари ва иловаларидан фойдаланиш;

i) файллардан фойдаланиш ва фойдаланиш тури;

j) тармоқ адреслари ва баённомалари;

k) фойдаланишни бошқариш тизимидан чиқадиган хабарлар;

l) муҳофаза қилиш тизимини, масалан, антивирус муҳофазаси ва бузиб киришларни аниқлаш тизимларини активация ва деактивация қилиш.

Бошқалар

Аудит журналлари бузиб киришлар тўғрисидаги маълумотларга ва шахсий конфиденциал маълумотларга эга бўлиши мумкин. Конфиденциалликни муҳофаза қилиш бўйича тегишли чоралар кўрилиши керак (15.1.4). Мумкин бўлган жойларда, тизим маъмурлари ўзларининг ҳаракатлари баённомаларини ўчиришлари ёки деактивация қилишлари ман этилади (10.1.3).

10.10.2 Тизимлардан фойдаланиш мониторинги

Бошқариш воситаси

Ахборотга ишлов бериш воситаларидан фойдаланиш мониторинги тартибини тасдиқлаш, шунингдек, мониторинг натижаларини мунтазам кўриб чиқиш зарур.

Жорий этиш бўйича қўлланма

Ахборотга ишлов бериш муайян воситаларининг мониторинги даражасини хавфларни баҳолаш асосида аниқлаш керак. Ташкилот кузатиб бориш бўйича ўзининг хатти-ҳаракатларига тегишли юридик талабларни бажариши керак. Мониторингда қуйидагиларга эътибор бериш керак:

a) рухсат берилган, жумладан қуйидаги деталларни ҳисобга олган фойдаланиш;

1) фойдаланувчининг идентификатори;

2) асосий воқеалар санаси ва вақти;

3) воқеалар турлари;

4) фойдаланиш амалга оширилган файллар;

5) фойдаланиладиган дастурлар/утилитлар;

b) қуйидагилар каби барча имтиёзли амаллар:

1) имтиёзли ҳисобга олинадиган ёзувлардан фойдаланиш, масалан, қўлланмалар, тизим маъмури ва маъмурнинг ёзувларидан;

2) тизимни ишга тушириш ва тўхтатиш;

3) киритиш/чиқариш қурилмасини улаш/узиш;

c) қуйидагилар каби рухсат берилмаган фойдаланишга уринишлар;

1) фойдаланувчиларнинг муваффақиятсиз ёки рад этилган хатти-ҳаракатлари;

2) ушбу ва бошқа активларга тегишли муваффақиятсиз ёки рад этилган хатти-ҳаракатлар;

3) фойдаланиш сиёсатининг ва тармоқ шлюзлари ҳамда тармоқлараро экранлар учун хабарномаларнинг бузилиши;

4) бузиб киришларни аниқлашнинг ўз тизимларидан огоҳлантириш;

d) қуйидагилар каби огоҳлантиришлар ёки тўхтаб қолишлар;

1) консол (терминал) огоҳлантиришлар ёки хабарлар;

2) тизимли рўйхатга олиш журналларида ёзилган истиснолар;

3) тармоқни бошқариш билан боғлиқ огоҳлантирувчи сигналлар;

e) тизимнинг созлаш ва хавфсизлигини бошқариш воситаларини ўзгартириш ёки ўзгартиришга уринишлар.

Кузатиш бўйича хатти-ҳаракатлар натижалари мониторингининг частотаси ўзаро аниқланган хавфларга боғлиқ бўлиши керак. Бунда ҳисобга олиниши керак бўлган хавф омиллари ўз ичига қуйидагиларни олади:

a) бизнес иловалар томонидан сақлаб туриладиган жараёнларнинг критиклиги;

b) амалдаги ахборотнинг аҳамияти, конфиденциаллиги ва сезгирлиги;

c) илгари бўлиб ўтган бузиб кириш ҳодисалари ва тизимдан нотўғри фойдаланишнинг таҳлили, шунингдек, заифликлардан фойдаланишнинг частотаси;

d) ташкилот ахборот тизимларининг бошқа тармоқлар билан, айниқса, умумий фойдаланиш тармоқлари билан ўзаро боғлиқлик даражаси;

e) воқеаларни рўйхатга олиш воситаларини узиб қўйиш.

Бошқалар

Мониторинг процедураларидан фойдаланувчилар томонидан фақат рухсат этилган ҳаракатларни бажаришни кафолатлаш учун фойдаланиш зарур.

Аудит журналини таҳлил қилиш (кўриб чиқиш) тизим дучор бўлган таҳдидларни ва уларнинг келиб чиқиш сабабларини тушунишни назарда тутади. Ахборот хавфсизлигининг бузилиш инцидентлари юз берганда кейинги текширувларни талаб қилиши мумкин бўлган ҳодисалар 13.1.1-бандда келтирилган.

10.10.3 Рўйхатга олиш журналларининг ахборотларини муҳофаза қилиш

Бошқариш воситаси

Ҳодисаларни рўйхатга олиш воситалари ва рўйхатга олиш журналларининг ахборотини аралашишдан ва рухсат этилмаган фойдаланишдан муҳофаза қилиш керак.

Жорий этиш бўйича қўлланма

Ахборот хавфсизлигини бошқариш бўйича тадбирлар воситаларни рухсат берилмаган ўзгаришлар ва тўхтаб қолишлардан муҳофаза қилишни таъминлаши керак, жумладан:

a) рўйхатга олинган хабарлар турларини ўзгартиришдан;

b) аудит журналлари таркибидаги файлларни таҳрир қилиш ёки йўқ қилишдан;

c) журналлар файллари жойлашган ёхуд воқеаларни ёзишни рад этишга ёхуд аввал рўйхатга олинган воқеаларни қайта ёзишга олиб келадиган ташувчиларнинг етарли бўлмаган сиғимидан.

Айрим аудит журналларига ҳужжатларни сақлаш сиёсатининг бир қисми сифатида ёки далилларни йиғиш ва сақлаш талабларига кўра, архивлаштириш талаблари қўйилиши мумкин (13.2.3).

Бошқалар

Аудитнинг тизим журналлари кўпинча хавфсизлик мониторинги нуқтаи назаридан қизиқиш уйғотмайдиган катта ҳажмдаги ахборотга эга бўлади. Хавфсизлик мониторингида катта аҳамиятга эга бўлган ҳодисаларни идентификация қилишни енгиллаштириш учун хабарларнинг тегишли турларидан алоҳида журналга автоматик нусха кўчириш имкониятини кўриб чиқиш ёки тўғри келадиган тизим утилитларидан ёки маълумотларни таҳлилга тайёрлаш учун аудитнинг инструментал воситалардан фойдаланиш мақсадга мувофиқ.

Тизим журналлари муҳофаза қилиниши керак, чунки улардаги маълумотларни ўзгартириш ёки йўқ қилиш мумкин бўлса, унда журналларнинг мавжудлиги хавфсизликнинг соҳта туйғусини келтириб чиқариши мумкин.

10.10.4 Маъмурлар ва операторларнинг хатти-ҳаракатларини рўйхатга олиш журналлари

Бошқариш воситаси

Тизим маъмури ва тизим операторининг хатти-ҳаракатларини рўйхатга олиш керак.

Жорий этиш бўйича қўлланма

Журналлар қуйидагиларни ўз ичига олиши керак:

a) ҳодиса юз берган вақт (муваффақиятли ёки муваффақиятсиз уриниш);

b) ҳодиса (масалан, ишлов берилган файллар) ёки тўхтаб қолиш (масалан, хато юз берди ва тузатувчи амал қўлланади) тўғрисидаги маълумот;

c) қандай ҳисобга олувчи ёзув ва қандай маъмур ва оператор жалб этилган;

d) қандай жараёнлар амалда бўлган.

Тизим маъмурлари ва операторларининг журналларини мунтазам текшириб туриш керак.

Бошқалар

Тизимли ва тармоқли маъмурий бошқариш бўйича хатти-ҳаракатларнинг қабул қилинган нормаларга мувофиқлигини кузатиб бориш учун тизим ва тармоқ маъмурлари етиши мумкин бўлган зонадан ташқарида бошқариладиган бузиб киришларни аниқлаш тизимидан фойдаланиш мумкин.

10.10.5 Тўхтаб қолишларни рўйхатга олиш

Бошқариш воситаси

Тўхтаб қолишларни рўйхатга олиш ва таҳлил қилиш, шунингдек, тегишли чоралар кўриш керак.

Жорий этиш бўйича қўлланма

Фойдаланувчилар ёки тизим дастурлари хабар берган, шунингдек, ахборотга ишлов бериш тизимлари ёки телекоммуникациялар тизимлари билан боғлиқ тўхтаб қолишларни рўйхатга олиш керак. Ушбу тўхтаб қолишлар билан муомалада бўлишнинг аниқ баён қилинган қоидаларини ўрнатиш керак, жумладан:

a) тўхтаб қолишлар оқибатларини муваффақиятли бартараф этиш учун тўхтаб қолишлар журналларини таҳлил қилиш;

b) бошқариш воситалари ошкор этилмаганлиги ва бажарилган хатти-ҳаракатларга тўлиқ рухсат берилганлигига ишонч ҳосил қилиш учун тузатиш киритувчи тадбирларни таҳлил қилиш.

Агар ушбу тизим функциясидан фойдаланиш мумкин бўлса, ҳодисаларни рўйхатга олиш киритилганлигига ишонч ҳосил қилиш керак.

Бошқалар

Хатоларни ва тўхтаб қолишларни рўйхатга олиш тизимнинг унумдорлигига таъсир қилиши мумкин. Бундай рўйхатга олишни ваколатли ходим киритиши, муайян тизимлар учун талаб қилинадиган ҳодисаларни рўйхатга олиш даражасини эса, унумдорлик пасайишини ҳисобга олиб, хавфларнинг таърифига мувофиқ белгилаш керак.

10.10.6 Соатларни синхронизация қилиш

Бошқариш воситаси

Ахборотга ишлов бериш барча тизимларининг соатлари, зарурат бўлганда, ташкилот доирасида ёки хавфсизлик соҳасида тегишли аниқ вақт манбаи билан синхронизация қилинган бўлиши керак.

Жорий этиш бўйича қўлланма

Компьютер ёки алоқа воситаси соатдан реал вақтда фойдаланиш имкониятига эга бўлган жойларда уларни мувофиқлаштирилган бутунжаҳон вақти (Universal Coordinated Time UCT) ёки маҳаллий стандарт вақт бўйича белгилаш керак. Маълумки, баъзи соатлар «олдин юради» ёки «орқада қолади», шунинг учун сезиларли ўзгаришларни текширадиган ва тўғрилайдиган процедура бўлиши керак.

Сана/вақтни тўғри акс эттириш учун сана/вақт форматини тўғри интерпретацияси таъминланиши муҳим. Ўзига хос маҳаллий хусусиятларни эътиборга олиш керак (масалан, ёзги ва қишки вақт).

Бошқалар

Компьютер соат (таймер)ларини тўғри ўрнатиш аудит журналларини тўлдиришнинг аниқлигини таъминлаш учун муҳим, бу журналлар текширувлар учун ёки суд ёки маъмурий терговларда далил сифатида керак бўлиши мумкин. Аудитнинг нотўғри журналлари бундай текширувларни қийинлаштириши, шунингдек, йиғилган исботларнинг ишончлилигидан шубҳаланишга олиб келиши мумкин. Рўйхатга олиш тизимлари учун асосий соат тариқасида аниқ вақт радиосигнали билан боғлиқ бўлган миллий атом соатларидан фойдаланиш мумкин.

Серверларнинг асосий соат билан синхронизация қилинишини таъминлаш учун вақтинчалик тармоқ баённомасидан фойдаланиш мумкин.

11 Фойдаланишни бошқариш

11.1 Мантиқий фойдаланишни бошқариш бўйича талаблар

Мақсад: ахборотдан фойдаланишни бошқариш.

Ахборотдан, ахборотга ишлов бериш воситаларидан ва бизнес-жараёндан фойдаланишни хавфсизлик ва бизнес талаблари асосида бошқариш керак.

Фойдаланишни бошқариш талаблари ахборотни тарқатиш ва авторизация қилишга тегишли қисмидаги сиёсатларда акс эттирилиши керак.

11.1.1 Фойдаланишни бошқариш сиёсати

Бошқариш воситаси

Фойдаланишни бошқариш сиёсатини бизнес ва хавфсизлик талаблари асосида аниқлаш, ҳужжатли расмийлаштириш ва қайта кўриб чиқиш керак.

Жорий этиш бўйича қўлланма

Фойдаланишни бошқариш сиёсатида фойдаланишни бошқариш қоидалари ва ҳар бир фойдаланувчи ёки фойдаланувчилар гуруҳи учун ҳуқуқлар аниқ ифодаланиши керак. Фойдаланишни бошқариш воситалари мантиқий ва жисмоний бўлади (9) ва уларни бирга кўриб чиқиш керак. Фойдаланувчилар ва хизматларни тақдим этувчилар бизнеснинг мантиқий ва жисмоний фойдаланишга тегишли талабларни бажариш зарурлиги тўғрисида хабардор бўлишлари керак.

Сиёсатда қуйидагилар ҳисобга олинган бўлиши зарур:

a) муайян бизнес-иловаларнинг хавфсизлик талаблари;

b) у дуч келадиган бизнес-иловалар ва хавфларнинг ишлаши билан боғлиқ барча ахборотни идентификация қилиш;

c) ахборотни тарқатиш ва фойдаланишни авторизация қилиш шартлари, масалан, фойдаланувчи фақат унга муайян вазифани бажариш учун зарур бўлган маълумотлардан, шунингдек, ахборотни таснифлаш ва уни муҳофаза қилишнинг талаб қилинган даражаларидан фойдаланиш ҳуқуқини олади (7.2);

d) фойдаланишни бошқариш бўйича сиёсатлар билан ахборот таснифи ўртасидаги мувофиқликни турли тизимлар ва тармоқларга татбиқ қилиниши.

e) маълумотлар ёки сервислардан фойдаланишни муҳофаза қилишга тегишли мавжуд қонун ҳужжатлари ва ҳар қандай шартнома мажбуриятлари (15.1);

f) фойдаланувчиларнинг ташкилотдаги бир типдаги мажбуриятлари ва жавобгарлиги учун фойдаланишнинг стандарт профиллари;

g) тақсимланган тармоқда фойдаланиш мумкин бўлган уланишларнинг барча турларини ҳисобга олган ҳолда фойдаланиш ҳуқуқларини бошқариш;

h) фойдаланишни бошқариш ролларини бўлиб бериш, масалан фойдаланиш учун талаб, фойдаланишга рухсат бериш, фойдаланишни маъмурий бошқариш;

i) фойдаланиш учун талабларга расмий рухсат бериш талаблари (11.2.1);

j) фойдаланишни бошқариш воситаларини даврий равишда қайта кўриб чиқиш талаблари (11.2.4);

k) фойдаланиш ҳуқуқини олиб қўйиш (8.3.3).

Бошқалар

Фойдаланишни бошқариш қоидаларини белгилашда қуйидагиларни эътиборга олиш керак:

a) муайян шароитларда қўлланадиган ёки шартли ҳисобланган, бажарилиши мажбурий бўлган қоидалар билан бажарилиши мажбурий бўлмаган қоидалар ўртасидаги фарқлар;

b) «ошкора тақиқланмагунча, умуман барча нарсага рухсат берилган» деган бўш принципга эмас, «ошкора рухсат берилмагунча, умуман барча нарса тақиқланган бўлиши керак» деган фикрга асосланган қоидаларни ифодалаш;

c) ахборотга ишлов бериш воситалари ёрдамида автоматик тарзда генерация қилинадиган ва фойдаланувчиларнинг ихтиёри бўйича инициация қилинадиган ахборот махфийлик грифларининг ўзгаришлари (7.2);

d) ахборот тизими томонидан автоматик равишда белгиланадиган ва маъмур томонидан белгиланган фойдаланувчи ҳуқуқларининг ўзгаришлари;

e) амалга киритишдан олдин махсус келишувни талаб қиладиган ва талаб қилмайдиган қоидалар.

Фойдаланишни бошқариш қоидаларини расмий тартиб ва аниқ белгиланган мажбуриятлар ёрдамида ўрнатиш мумкин (6.1.3, 11.3, 10.4 1, 11.6).

11.2 Фойдаланувчиларнинг кира олишини бошқариш

Мақсад: Ахборот тизимларидан рухсат берилган фойдаланишни таъминлаш ва рухсатсиз фойдаланишнинг олдини олиш.

Ахборот тизимлари ва хизматларидан фойдаланиш ҳуқуқларини тақсимлашни бошқариш расмий тартибининг мавжудлигини таъминлаш керак.

Тартиб тизимда янги фойдаланувчиларни рўйхатдан ўтказишдан бошлаб ва ахборот тизимлари ва сервисларидан бошқа фойдаланиш керак

бўлмаган фойдаланувчиларнинг ҳисобга олинган ёзувларини йўқ қилишгача бўлган фойдаланувчилар кира олишлари ҳаётий циклининг барча стадияларини қамраб олиши зарур. Алоҳида эътиборни имтиёзли фойдаланиш ҳуқуқларини тақдим этишга тегишли тадбирларга қаратиш керак. Фойдаланувчилар уларнинг ёрдамида тизимнинг назорат воситаларини айланиб ўтиши мумкин.

11.2.1 Фойдаланувчиларни рўйхатга олиш

Бошқариш воситаси

Барча ахборот тизимлари ва хизматларидан фойдаланишни тақдим этиш ва олиб қўйиш учун фойдаланувчиларнинг ҳисобга олинган ёзувларини рўйхатга олиш ва йўқ қилишнинг расмий тартиби амал қилиши керак.

Жорий этиш бўйича қўлланма

Фойдаланишни бошқариш процедураси фойдаланувчиларни рўйхатга олишда ва рўйхатга олишни бекор қилишда қуйидагиларни ўз ичига олиши керак:

a) ноёб идентификаторлар ёки фойдаланувчилар номларидан шундай фойдаланиш керакки, фойдаланувчилар тизимга киришлари ва ўз хатти-ҳаракатлари учун жавоб беришлари мумкин бўлсин; гуруҳли идентификаторлардан фойдаланишга фақат бизнес учун ёки эксплуатацион сабабларга кўра зарур бўлган ҳолларда йўл қўйилади, бинобарин бунга рухсат берилган ва ҳужжатлаштирилган бўлиши керак;

b) фойдаланувчи тизим маъмури томонидан ахборот тизимлари ва сервислардан фойдаланиш учун авторизация қилинганлигини текшириш. Бундан ташқари, раҳбариятдан ҳуқуқларни тақдим этиш учун қўшимча рухсат олиш мақсадга мувофиқ бўлиши мумкин;

c) ташкилот хавфсизлик сиёсатининг талабларини, масалан, мажбуриятларни бўлиш принципини (10.1.3) ҳисобга олган ҳолда, фойдаланишнинг тақдим этилган даражасининг ишлаб чиқариш заруратига мувофиқлигини текшириш (11.1);

d) фойдаланувчиларга уларнинг фойдаланиш ҳуқуқлари кўрсатилган ёзма ҳужжатни тақдим этиш;

e) фойдаланувчиларни уларга тақдим этилган фойдаланиш ҳуқуқлари билан имзо қўйдириб таништириш;

f) авторизация қилиш процедуралари тугамагунча хизматларни етказиб берувчилар фойдаланишни тақдим этмасликларига ишонч ҳосил қилиш;

g) сервислардан фойдаланадиган барча рўйхатга олинган шахсларнинг тегишли расмий ҳисобини юритиш;

h) лавозим мажбуриятлари ўзгарган ёки ташкилотдан бўшаб кетган фойдаланувчиларнинг фойдаланиш ҳуқуқларини дарҳол бекор қилиш;

i) фойдаланувчиларнинг ортиқча идентификаторлари ва ҳисобга олиш ёзувларини вақти-вақти билан текшириш ва йўқ қилиш (11.2.4);

j) фойдаланувчиларнинг ортиқча идентификаторлари бошқа фойдаланувчиларга берилмаганлигини текшириш.

Бошқалар

Фойдаланувчига фойдаланиш ҳуқуқларини тақдим этиш бизнес талаблари, шунингдек, фойдаланишнинг кўпгина ҳуқуқларини жамловчи фойдаланишнинг намунавий профилларига асосланган бўлиши керак. Фойдаланиш эҳтиёжлари ва қайта кўрилиши (11.2.4) муайян ҳуқуқлар даражасига қараганда, ушбу даражада осон бошқарилади.

Рухсатсиз фойдаланишга уриниш ҳолларида тегишли санкциялар қўлланиши тўғрисидаги қоидаларни ходимларнинг меҳнат шартномаларига ва хизматларни етказиб берувчилар билан тузиладиган контрактларга киритиш имконини кўриб чиқиш зарур (6.1.5, 8.1.3, 8.2.3).

11.2.2 Имтиёзларни бошқариш

Бошқариш воситаси

Имтиёзларни белгилаш ва улардан фойдаланиш чекланган ва бошқариладиган бўлиши керак.

Жорий этиш бўйича қўлланма

Рухсатсиз фойдаланишдан муҳофаза қилишни талаб қиладиган кўп фойдаланиладиган тизимларда имтиёзларни тақдим этиш авторизация қилишнинг расмийлаштирилган жараёни ёрдамида назорат қилиниши зарур. Бунда қуйидаги тадбирларни қўллаш мақсадга мувофиқ:

a) ҳар бир тизим маҳсулотига, масалан, операцион тизим, маълумотлар базаси ва ҳар бир бизнес-иловани бошқариш тизимларига, шунингдек, ушбу имтиёзлар берилиши керак бўлган ходимлар тоифасига тегишли имтиёзларни идентификация қилиш;

b) имтиёзлар фойдаланувчиларга фойдаланишни бошқариш сиёсатига мувофиқ (11.1.1) «зарур фойдаланиш» принципи ва «ҳодиса ортидан ҳодиса» принципи асосида ишлаш учун зарур бўлган ходимларга ва фақатгина иш бажариш вақтида бунга эҳтиёж пайдо бўлганда тақдим этилиши керак;

c) барча берилган имтиёзларни авторизация қилиш ва рўйхатдан ўтказиш жараёнини таъминлаш зарур. Имтиёзлар авторизация қилиш жараёни тугатилмасдан берилиши керак эмас;

d) фойдаланувчиларга қўшимча имтиёзларни бериш заруратидан мустасно бўлиш учун стандарт тизим утилитлари (скриптлари)ни ишлаб чиқиш ва улардан фойдаланиш сиёсатини олиб бориш керак;

e) иш учун имтиёзлардан фойдаланишни талаб қилмайдиган ишлаб чиқиш ва дастурлардан фойдаланишга ёрдам бериш керак;

f) кундалик режимда ишлаганда ва имтиёзлардан фойдаланилганда фойдаланувчиларнинг турли идентификаторларидан фойдаланиш керак.

Бошқалар

Кўп фойдаланиладиган ахборот тизимларининг (фойдаланувчига тизимнинг назорат воситаларини ёки бизнес иловаларни четлаб ўтишга имкон берадиган) воситаларини қўллашда имтиёзларни тақдим этиш ва

улардан фойдаланишни чеклаш ва назорат қилиш зарур, чунки имтиёзлардан ноадекват фойдаланиш кўпинча тизимлар тўхтаб қолишининг асосий сабаби бўлади.

11.2.3 Фойдаланувчилар паролларини бошқариш

Бошқариш воситаси

Паролларни тақдим этиш бошқаришнинг расмий жараёни орқали назорат қилиниши керак.

Жорий этиш бўйича қўлланма

Ушбу жараён қуйидагиларни кўзда тутиши керак:

a) фойдаланувчилар томонидан шахсий паролларининг тўлиқ конфиденциаллигига риоя қилиш, гуруҳ пароллари борасида эса - ишчи гуруҳ даврасида конфиденциалликка риоя қилиш зарурлиги тўғрисидаги ҳужжатни имзолаш. Ушбу имзоланган контракт меҳнат шартномасининг шартларига киритилиши мумкин (8.1.3);

b) фойдаланувчилардан ўз паролларини бошқариш талаб қилинган ҳолларда, фойдаланувчини тизимда биринчи рўйхатдан ўтказишда алмаштиришга мажбур қиладиган хавфсиз бирламчи вақтинчалик пароль тақдим этилиши таъминланиши зарур (11.3.1);

c) янги ёки вақтинчалик пароль тақдим этилишидан ёхуд уни ўзгартиришдан олдин фойдаланувчининг шахсини аниқлаш тартибини тасдиқлаш;

d) вақтинчалик паролларни фойдаланувчиларга хавфсиз усулда бериш керак; паролларни воситачи орқали ёки электрон почтанинг муҳофазаланмаган (очиқ матн билан) хабарлари орқали беришдан қочиш керак;

e) вақтинчалик пароллар ҳар бир шахс учун такрорланмаслиги ва тахмин қилиб билиб олинадиган бўлмаслиги керак;

f) фойдаланувчилар паролларни олганликларини тасдиқлашлари керак;

g) паролларни компьютер тизимларида муҳофазаланмаган шаклда сақлаш керак эмас;

h) тизимлар ёки дастурий таъминот ўрнатилганидан сўнг етказиб берувчилар паролларини олдиндан белгилаб қўйиш бўйича ўзартириш керак.

Бошқалар

Пароллар ахборот тизими ёки сервисдан фойдаланишда фойдаланувчининг шахсини тасдиқлашнинг энг кенг тарқалган воситаларидан ҳисобланади. Заруратга қараб, фойдаланувчини идентификация ва аутентификация қилиш учун биометрия (бармоқ изларига қараб ҳақиқийлигини текшириш ва ш.к.), имзонинг ҳақиқийлигини текшириш ва аппарат воситаларидан, масалан смарт-картадан фойдаланиш каби бошқа технологияларнинг имкониятларини кўриб чиқиш керак. Зарурат бўлганда улардан фойдаланишни кўриб чиқиш керак.

11.2.4 Фойдаланувчиларнинг кира олиш ҳуқуқларини қайта кўриб чиқиш

Бошқариш воситаси

Раҳбарият расмий жараёндан фойдаланиб, фойдаланувчиларнинг кира олиш ҳуқуқларини мунтазам қайта кўриб чиқиши керак.

Жорий этиш бўйича қўлланма

Кира олиш ҳуқуқларини қайта кўриб чиқишда қуйидаги тавсияларни кўриб чиқиш керак:

a) фойдаланувчиларнинг кира олиш ҳуқуқлари мунтазам (тавсия қилинадиган давр - 6 ой) ва ҳар қандай хизмат бўйича кўтарилиш, лавозимини пасайтириш ёки меҳнат шартномасини бекор қилиш каби ўзгаришлардан сўнг қайта кўриб чиқилиши керак (11.2.1);

b) фойдаланувчиларнинг кира олиш ҳуқуқларини қайта кўриб чиқиш ва ташкилот ичида бир лавозимдан бошқасига ўтказишда қайта белгилаш керак;

c) фойдаланишнинг махсус имтиёзли ҳуқуқларини авторизация қилиш (11.2.2) кам вақт оралиғидан сўнг амалга оширилиши керак (тавсия қилинадиган давр - 3 ой);

d) авторизация қилинмаган имтиёзлар олинмаганлигига ишонч ҳосил қилиш учун берилган имтиёзлар вақти-вақти билан текширилиши керак;

e) имтиёзли ҳисобга олиш ёзувларидаги ўзгаришларни вақти-вақти билан назорат қилиш учун рўйхатга олиш керак.

Бошқалар

Маълумотлар ва ахборот хизматларидан фойдаланишни самарали бошқаришни таъминлаш учун фойдаланувчиларнинг кира олиш ҳуқуқларини мунтазам қайта кўриб чиқиш зарур.

11.3 Фойдаланувчиларнинг мажбуриятлари

Мақсад: фойдаланувчиларнинг рухсатсиз фойдаланишининг, ахборот ва унга ишлов бериш воситаларининг компрометация қилиниши ёки ўғирланишининг олдини олиш.

Авторизация қилинган фойдаланувчиларнинг ўзаро ҳаракати хавфсизлик самарадорлигининг муҳим жиҳати ҳисобланади.

Кира олишни бошқаришнинг, хусусан, пароллардан фойдаланиш ва ускунанинг хавфсизлигига нисбатан самарали механизмларини таъминлаш учун ўзларининг жавобгарликлари тўғрисида хабардор бўлишлари зарур.

Рухсатсиз фойдаланиш ёки қоғозлар, ташувчилар ва ахборотга ишлов бериш воситаларининг шикастланиш хавфини камайтириш учун тоза стол ва тоза экран сиёсатини жорий этиш керак.

11.3.1 Паролларлан фойдаланиш

Бошқариш воситаси

Фойдаланувчилар паролларни танлашда ва улардан фойдаланишда хавфсизликни таъминлашнинг белгиланган қоидаларига амал қилишлари керак.

Жорий этиш бўйича қўлланма

Барча фойдаланувчилар қуйидагиларнинг зарурлиги тўғрисида хабардор бўлишлари керак:

a) паролларнинг конфиденциаллигини сақлаш;

b) агар паролларнинг ишончли сақланиши таъминланмаган ва сақлаш методи тасдиқланган бўлса, паролларни ёзишни ман этиш (масалан, қоғозда, дастурлар файллари ёки кўчма қурилмаларда);

c) ҳар гал тизим ёки паролнинг мумкин бўлган компрометация қилиниши белгилари пайдо бўлганда паролларни ўзгартириш;

d) етарли минимал узунликдаги қуйидаги сифатли паролларни танлаш:

1) осон эсда қоладиган;

2) пароль эгаси билан боғлиқ, масалан, исмлар, телефон номерлари, туғилган саналар ва ҳ. шахсий маълумотларидан фойдаланганда осон топиб ёки ҳисоблаб бўлмайдиган;

3) луғат бўйича ҳужумларга заиф бўлмаган (яъни луғатларга киритилган сўзлардан ташкил топмаган);

4) ўхшаш белгиларнинг кетма-кетлиги саналмаган ва фақат рақамли ёки фақат ҳарфли гуруҳдан иборат кетма-кетлик бўлмаган;

e) паролларни тенг вақт оралиғида ёки фойдаланишларнинг маълум сонидан сўнг ва эски пароллардан қайта ёки даврий равишда фойдаланишдан воз кечгандан сўнг ўзгартириш (ҳисобга олинган имтиёзли ёзувларнинг паролларини оддий паролларга қараганда тез-тез алмаштириш керак);

f) вақтинчалик паролларни тизимда биринчи бор рўйхатдан ўтказганда ўзгартириш;

g) паролларни рўйхатдан ўтказишнинг автоматик жараёнига киритишни ман этиш, масалан, сақланадиган макрокомандалар ёки функционал клавишалардан фойдаланиб;

h) индивидуал пароллардан коллектив бўлиб фойдаланишдан мустасно бўлиш;

i) битта паролдан хизматга оид ва хизматдан ташқари мақсадлар учун фойдаланмаслик.

Агар фойдаланувчилар кўп сонли хизматлардан ёки бизнес-иловалардан фойдаланиш эҳтиёжига эга бўлсалар ва кўп сонли паролларни ишлатишга мажбур бўлсалар, барча сервислар учун ҳар бир тизим ва платформада сақланадиган паролни муҳофаза қилишнинг оқилона даражасини таъминлайдиган битта сифатли паролни (11.3.1.d) ишлатиш мумкинлигини тавсия қилиш мумкин.

Бошқалар

Таъминлаш тизимли хизматининг раҳбарияти йўқотилган ёки унутилган пароллар тўғрисидаги буюртмага ишлов беришда айниқса эҳтиёткорликка риоя қилишлари керак, чунки таъминлаш хизматига мурожаат қилиш ҳам, шунингдек, пароллар тизимига ҳужум қилиш воситаси бўлиши мумкин.

11.3.2 Фойдаланувчилар томонидан қаровсиз қолдирилган ускуналар

Бошқариш воситаси

Фойдаланувчилар қаровсиз қолдирилган ускунанинг муносиб муҳофазасини таъминлашлари керак.

Жорий этиш бўйича қўлланма

Барча фойдаланувчилар ва пудратчилар хавфсизлик талаблари ва қаровсиз қолдирилган ускунани муҳофаза қилиш методларини, шунингдек, ана шундай муҳофазани таъминлаш бўйича ўз мажбуриятларини билишлари керак. Фойдаланувчиларга қуйидагилар тавсия этилади:

a) агар блокировкалаш механизми, масалан, пароль билан муҳофазаланган экранни сақловчи бўлмаса, иш охирида актив сеансларни якунлаш;

b) марказий процессор билан алоқа сеанси тугаганда тизимдан чиқиш процедурасини бажариш (яъни фақат компьютер ва терминални ўчириш билан кифояланмаслик);

c) фойдаланилмайдиган компьютерлар ёки терминалларни рухсатсиз фойдаланишдан калит билан қулфланадиган қулф ёки эквивалент назорат воситаси ёрдамида муҳофаза қилиш, масалан, кириш паролини ўрнатиш йўли билан (11.3.3).

Бошқалар

Ишга оид зоналарда ўрнатилган ускуна, масалан, ишчи станциялар ёки файлли серверлар узоқ вақт қаровсиз қолдирилганда рухсатсиз фойдаланишдан махсус муҳофаза қилишни талаб қиладилар.

11.3.3 «Тоза стол» ва «тоза экран» сиёсати

Бошқариш воситаси

Қоғоз ҳужжатлар ва ахборотнинг электрон ташувчиларига тегишли «тоза стол» сиёсатини ва ахборотга ишлов бериш воситаларига тегишли «тоза экран» сиёсатини қўллаш керак.

Жорий этиш бўйича қўлланма

«Тоза стол» ва «тоза экран» сиёсати ахборот таснифини (7.2), юридик ва шартномавий талабларни (15.1), шунингдек ташкилотда қабул қилинган тегишли хавфларни ва этик нормаларни ҳисобга олиши керак. Қуйидаги тавсияларни кўриб чиқиш зарур:

a) ахборот компрометация қилинишидан мустасно бўлиш учун ахборотнинг қоғоз ва электрон ташувчиларидан фойдаланилмаганда, уларни тегишли қулфланадиган шкафларда ва/ёки мебелнинг

муҳофазаланган предметларида сақлаш керак, айниқса, ишдан ташқари вақтда;

b) қаровсиз қолдирилган компьютер ёки терминаллар тизимга кириш режимида турмаслиги керак ёки фойдаланувчининг пароль, токен, бошқа шунга ўхшаш аутентификация қилиш механизми билан бошқариладиган экран ва клавиатуранинг блокировкалаш механизмлари билан муҳофазаланган бўлиши керак. Компьютер ёки терминалдан фойдаланиш жараёнида танаффус бўлган ҳолда муҳофазани клавиатура қулфлари, пароллар ёки бошқа бошқариш воситалари билан амалга ошириш керак.

c) хат-хабарларни жўнатиш/қабул қилиш пунктлари, шунингдек, факсимиль ва телекс аппаратлари қаровсиз қолдирилганда муҳофаза қилиниши таъминланиши зарур;

d) фотонусха кўчириш ва бошқа қайта ишлаб чиқарадиган қурилмалардан (масалан, сканерлар, рақамли камералар) рухсатсиз фойдаланишнинг олдини олиш керак;

e) конфиденциал ёки грифланган ахборотга эга бўлган босиб чиқарилган ҳужжатларни принтерлардан дарҳол чиқариб олиш керак.

Бошқалар

«Тоза стол» ва «тоза экран» сиёсати иш вақтида ва ишдан ташқари вақтда рухсатсиз фойдаланиш, ахборотни иш вақтида ва ишдан ташқари вақтда йўқотиш ва шикастланиш хавфларини камайтиради. Сейфлар ва сақлаш хавфсиз воситаларининг бошқа турлари, шунингдек, уларда сақланадиган ахбортни ёнғин, ер қимирлаши, сув тошиши ёки портлаш каби офатлардан муҳофаза қилиши мумкин.

Босиб чиқарилган нусхаларни фақат уларнинг яратувчилари томонидан ва фақат принтер ёнида бўлганларида олинишини таъминловчи пин-кодлар функциясига эга бўлган принтерлардан фойдаланиш тавсия этилади.

11.4 Тармоқдан фойдаланишни бошқариш

Мақсад: тармоқ сервисларидан рухсатсиз фойдаланишнинг олдини олиш.

Ички тармоқ сервисларидан фойдаланиш каби, ташқи тармоқ сервисларидан фойдаланиш ҳам бошқариладиган бўлиши керак.

Тармоқ ва тармоқ сервисларидан фойдаланувчиларнинг кириши қуйидагиларни таъминлаш билан уларнинг хавфсизлигини компрометация қилмаслиги керак:

a) ташкилот тармоғи ва бошқа ташкилотлар тармоқлари ёки умумий фойдаланиш тармоқлари ўртасидаги тегишли интерфейслар;

b) фойдаланувчилар ва ускуна учун аутентификация қилишнинг тегишли механизмлари;

c) фойдаланувчиларнинг ахборот сервисларидан фойдаланишини бошқариш.

11.4.1 Тармоқ сервисларидан фойдаланиш сиёсати

Бошқариш воситаси

Фойдаланувчиларнинг фақат уларга фойдаланиш рухсат берилган сервислардан бевосита фойдаланишини таъминлаш керак.

Жорий этиш бўйича қўлланма

Тармоқлар ва тармоқ сервисларидан фойдаланиш сиёсатини таърифлаш керак. Бунда қуйидагилар белгиланган бўлиши керак:

a) фойдаланиш рухсат берилган тармоқ ва тармоқ сервислари;

b) кимга, қайси тармоқ ва тармоқ сервисларидан фойдаланиш учун рухсат бериш тартиби;

c) тармоқ сервисларидан рухсатсиз фойдаланишдан муҳофаза қилиш бўйича тадбирлар ва процедуралар;

d) тармоқ ва тармоқ сервисларидан фойдаланиш учун ишлатиладиган воситалар (масалан, Интернет тармоғининг провайдери ёки узоқлаштирилган тизим билан коммутацияланадиган уланишга рухсат бериш шартлари).

Тармоқ сервисларидан фойдаланиш сиёсати фойдаланишни бошқариш бўйича бизнес сиёсатига қарши бўлмаслиги керак (11.1).

Бошқалар

Тармоқ сервислари билан рухсатсиз ва муҳофаза қилинмаган уланишлар бутун ташкилотга таъсир қилиши мумкин. Фойдаланишни бошқариш конфиденциал ёки муҳим критик бизнес-иловаларга тармоқ уланишлари учун, шунингдек, катта хавф остидаги зоналарда, масалан, жамоат жойларида ёки ташкилот чегараларидан ташқарида - ташкилот томонидан бевосита бошқариш ва хавфсизликни назорат қилиш соҳасидан ташқарида бўлган фойдаланувчилар учун айниқса зарур.

11.4.2 Ташқи уланишларда фойдаланувчиларни аутентификация қилиш

Бошқариш воситаси

Узоқдаги фойдаланувчиларнинг кира олишини бошқариш учун аутентификация қилишнинг тегишли методларидан фойдаланиш керак.

Жорий этиш бўйича қўлланма

Узоқдаги фойдаланувчиларни аутентификация қилишга криптографиядан, аппаратурани идентификация қилиш воситаларидан, ёки «жавоб-тақриз» методини қўллаб-қувватловчи баённомаларидан фойдаланилганда эришиш мумкин. Бундай методлар хусусий виртуал тармоқлар (virtual private notworks VPN)нинг турли ечимларида амалга оширилган. Уланишлар манбаига ишончни таъминлаш учун, шунингдек, ажратилган хусусий линиялар ёки фойдаланувчининг тармоқ адресини текшириш воситалари ҳам ишлатилиши мумкин.

Тескари чақирувни, масалан, тескари чақирувли модемлардан фойдаланишни назорат қилиш процедуралари ва воситалари ташкилот ахборотини қайта ишловчи воситаларга рухсатсиз ва исталмаган уланишлардан муҳофаза қилинишини таъминлаши мумкин, чунки

уларнинг ёрдамида ташкилот тармоғи билан узоқдаги алоқани ўрнатишга уринаётган фойдаланувчиларнинг фойдаланиш ҳуқуқи тасдиқланади. Ташкилотнинг ушбу усулларидан фойдаланишда чақирувни бошқа адресга улайдиган тармоқ сервисларидан фойдаланиш керак эмас. Агар улардан фойдаланилганда ҳам, бу билан боғлиқ хавфларни четлаб ўтиш учун бошқа адресга йўллаш имкониятларини блокировкалаб қўйиш керак. Шунингдек, тескари чақирув жараёни ҳақиқатда ташкилот томонида узилиш амалга оширилганлигига ишонч ҳосил қилишни таъминлаши муҳим. Акс ҳолда узоқдаги фойдаланувчи тескари чақирув текширувини соҳталаштириб линияни банд қилиб туриши мумкин. Шу каби инцидентларга йўл қўймаслик учун процедуралар ва тескари чақирув назорат воситаларини синчиклаб тестдан ўтказиш керак.

Узелни аутентификация қилиш биргаликда фойдаланиладиган хавфсиз компьютер ускунаси билан боғланадиган узоқдаги фойдаланувчилар гуруҳларининг муқобил аутентификация қилиш воситаси бўлиб хизмат қилиши мумкин. Узелни аутентификация қилиш учун криптографик методлардан, масалан, компьютерлар сертификатларига асосланган методлардан фойдаланиш мумкин. Бу VPN да асосланган баъзи ечимларнинг бир қисми ҳисобланади.

Симсиз тармоқлардан фойдаланишни бошқариш учун аутентификация қилишнинг қўшимча воситаларини жорий қилиш керак. Хусусан, яширин ҳолда тутиб олиш ва тармоқ трафиги киритмалари эҳтимоли катта бўлганлиги сабабли симсиз тармоқлар учун бошқариш воситаларини танлашда айниқса эҳтиёткорликка риоя қилиш керак.

Бошқалар

Ташқи уланишлар хизматга оид ахборотдан рухсатсиз фойдаланиш учун имкон беради, масалан, коммутация қилинадиган каналлардан фойдаланиш. Шунинг учун узоқдаги фойдаланувчиларга фойдаланишни тақдим этишда улар аутентификация қилинган бўлиши керак. Аутентификация қилишнинг баъзи методлари бошқаларига қараганда муҳофаза қилишнинг юқори даражасини таъминлайди. Масалан, криптографиядан фойдаланишга асосланган методлар ишончли аутентификация қилишни таъминлаши мумкин. Хавфни баҳолашдан келиб чиқиб, аутентификация қилишнинг тегишли методини танлаш учун муҳофазанинг талаб қилинган даражасини белгилаш муҳим.

Узоқлаштирилган компьютер билан автоматик уланиш воситаси бизнес-иловадан рухсатсиз фойдаланиш усулининг бирини тақдим этиши мумкин. Агар уланиш ташкилот хавфсизлигини бошқариш ва назорат қилиш зонасидан ташқаридаги тармоқдан фойдаланса, бу айниқса муҳим.

11.4.3 Тармоқларда ускунани идентификация қилиш

Бошқариш воситаси

Ускунани тизимнинг муайян нуқталарига уланишини аутентификация қилиш учун уни тармоқда автоматик идентификация қилиш имкониятини кўриб чиқиш керак.

Жорий этиш бўйича қўлланма

Фақат белгиланган жойлардан ёки белгиланган ускунадан алоқа ўрнатиш зарур бўлганда ускунани идентификация қилишдан фойдаланиш мумкин. Ускунага ўрнатилган ёки уланган идентификатор ушбу муайян ускунага инициация қилиш ёки маълум хабарларни олишга рухсат берилганлигини аниқлаш учун ишлатилиши мумкин. Бир нечта тармоқ мавжуд бўлганда ёки ушбу тармоқлар турли критикликка эга бўлса, ушбу идентификаторлар ускунага қайси тармоқ билан уланишга рухсат берилганлигини аниқ кўрсатиши керак. Тармоқда ускуна идентификаторининг хавфсизлигини таъминлаш учун жисмоний муҳофазани қўллаш керак бўлиб қолиши мумкин.

Бошқалар

Бошқаришнинг ушбу воситаси фойдаланувчилар ускунасини аутентификация қилишнинг бошқа методлари билан тўлдирилиши мумкин (11.4.2). Ускунани идентификация қилиш фойдаланувчилар аутентификациясига қўшимча равишда қўлланиши мумкин.

11.4.4 Узоқлаштирилган диагностик ва конфигурацион портларни муҳофаза қилиш

Бошқариш воситаси

Диагностик ва конфигурацион портлардан жисмоний ва мантиқий фойдаланишни бошқариш керак.

Жорий этиш бўйича қўлланма

Диагностик ва конфигурацион портларни бошқариш воситалари ўз ичига қулфлар ва жисмоний фойдаланишни бошқаришнинг ёрдамчи процедураларини олиши мумкин. Диагностик ва конфигурацион портлардан фойдаланишни компьютер сервисларини таъминлаш учун жавобгар ва техник хизмат кўрсатиш бўйича мутахассисларнинг фойдаланишини талаб қиладиган маъмур ўртасидаги келишувга мувофиқ таъминлаш бундай ёрдамчи процедуранинг мисоли бўлиши мумкин. Портлар, сервислар ва компьютерда ёки тармоқ қурилмасида ўрнатилган ва бизнеснинг муайян фаолияти учун талаб этилмаган бошқа ёрдамчи ускуна узиб қўйилиши ёки йўқ қилиниши керак.

Бошқалар

Кўпгина компьютер тармоқлари ва телекоммуникация тизимлари техник хизмат кўрсатувчи мутахассисларнинг фойдаланиши учун узоқлаштирилган диагностик воситалар тўпламига эга. Муҳофаза қилинмаган бу диагностик портлар рухсатсиз фойдаланиш хавфининг манбаси бўлиб ҳисобланади.

11.4.5 Тармоқларда ажратиш принципи

Бошқариш воситаси

Тармоқларда фойдаланувчилар ва ахборот тизимларининг ахборот хизматлари гуруҳларини ажратиш керак.

Жорий этиш бўйича қўлланма

Йирик тармоқлар хавфсизлигини бошқаришнинг методларидан бири уларни алоҳида мантиқий тармоқ доменларига, масалан, ҳар бири хавфсизликнинг белгиланган периметри билан муҳофазаланган, ташкилотнинг ички тармоқ домени ва ташқи тармоқ доменларига ажратишдан иборат. Тармоқ хавфсизлигининг муҳитларини кейинчалик ажратиш мақсадида турли мантиқий тармоқ доменларида бошқариш воситаларининг босқичли ўзгарадиган тўпламини қўллаш мумкин, масалан, ҳамма эркин фойдалана олиши мумкин бўлган тизимлар, ички тармоқлар ва сезгир активлар. Доменларни хавфларни аниқлаш ва ҳар бир домен доирасида хавфсизликнинг турли талаблари асосида аниқлаш керак.

Эсга олинган тармоқ периметри икки домен ўртасидаги фойдаланиш ва ахборот оқимини бошқариш мақсадида уланиши керак бўлгани икки тармоқ ўртасида хавфсиз шлюзни ўрнатиш йўли билан жорий этилиши мумкин. Ушбу шлюзни ташкилотнинг фойдаланишни бошқариш сиёсатига мувофиқ (11.1) доменлар ўртасидаги трафикни (11.4.6, 11.4.7) фильтрлаш учун ва рухсат берилмаган фойдаланишни блокировкалаш учун конфигурация қилиш керак. Тармоқлараро экран бундай шлюзнинг мисоли бўла олади.

Мантиқий доменларни ажратишнинг бошқа методи ташкилот ичида бир гуруҳ фойдаланувчилар учун хусусий виртуал тармоқлар ёрдамида тармоқдан фойдаланишни чеклашдан иборат.

Тармоқлар, шунингдек, тармоқ қурилмаларининг функционал имкониятлари, масалан, IP протоколи бўйича коммутация, ёрдамида ажратилган бўлиши мумкин. Бундай ҳолда ажратилган соҳалар маршрутлаш/коммутация қилиш имкониятларидан фойдаланилган ҳолда, фойдаланишни бошқариш рўйхатлари каби, тармоқ маълумотларининг оқимини бошқариш йўли билан жорий этилган бўлиши мумкин.

Тармоқларни доменларга ажратиш учун мезонларни фойдаланишни бошқариш сиёсатини таҳлил қилиш (11.1) асосида шакллантириш, шунингдек, ушбу ажратишнинг маршрутлашнинг тўғри келадиган методларини ёки тармоқ шлюзларини (11.4.6, 11.4.7) жорий қилиш натижасида унумдорликка таъсирини ҳисобга олиш керак.

Бундан ташқари, хизмат кўрсатишнинг мумкин бўлган бузилишига таъсирни минимумга келтириш мақсадида тармоқлардаги ажратишни ахборотнинг ишонч ва ихтисослаштириш даражасидаги тармоғида сақланадиган ва ишлов бериладиган нархи ва таснифида асослаш керак.

Симсиз тармоқларни ички тармоқлар ва умумий фойдаланиш тармоқларидан ажратишни кўриб чиқиш керак. Симсиз тармоқларнинг периметрлари аниқ белгиланмаганлиги учун бундай ҳолларда тармоқларни ажратишни таъминлаш учун бошқариш воситаларини аниқлаш мақсадида хавфларни аниқлаш керак (масалан, барқарор аутентификация, криптографик усуллар ва частотани танлаш).

Бошқалар

Ҳамкорликнинг янги турлари пайдо бўлиши ва тармоқ воситалари ҳамда ахборотга ишлов бериш восталаридан биргаликда фойдаланиш зарурати юзага келиши муносабати билан тармоқлар ташкилотнинг одатдаги чегарасидан ташқарига тарқалади.

Бундай кенгайиш конфиденциаллиги ва сезгирлиги туфайли бошқа фойдаланувчилардан муҳофаза қилиниши керак бўлиши мумкин бўлган баъзи мавжуд тармоқ ахборот тизимларидан рухсатсиз фойдаланиш хавфини оширади.

11.4.6 Тармоқ уланишларини назорат қилиш

Бошқариш воситаси

Биргаликда фойдаланиладиган, айниқса, ташкилот чегарасидан четга чиқадиган тармоқлар учун фойдаланишни бошқариш сиёсати ва бизнес иловаларининг талабларига мувофиқ фойдаланувчиларнинг тармоқ билан уланиш имкониятларини чеклаш керак (11.1).

Жорий этиш бўйича қўлланма

Фойдаланувчиларнинг тармоқдан фойдаланиш ҳуқуқини фойдаланишни бошқариш сиёсатига мувофиқ сақлаш ва янгилаш керак (11.11).

Фойдаланувчиларнинг улаш имкониятини трафикни олдиндан белгиланган муайян жадваллар ва қоидалар ёрдамида фильтрлайдиган тармоқ шлюзлари ёрдамида чеклаш мумкин. Чеклашлар қўлланиши керак бўлган бизнес-иловалар мисоллари:

a) хабарлар билан алмашинув, масалан, электрон почта хабарлари;

b) файлларни узатиш;

c) интерактив фойдаланиш;

d) амалий фойдаланиш.

Тармоқдан фойдаланиш ҳуқуқларини куннинг муайян вақти ёки саналари билан боғланишини кўриб чиқиш керак.

Бошқалар

Фойдаланишни бошқариш сиёсати биргаликда фойдаланиладиган тармоқлар, айниқса ташкилот чегарасидан четга чиқадиганлари учун фойдаланувчиларнинг имкониятларини чекловчи бошқариш воситаларини киритишни талаб қилиши мумкин.

11.4.7 Тармоқларда маршрутлашни бошқариш

Бошқариш воситаси

Бизнес-иловалар учун фойдаланишни бошқариш сиёсатининг бузилишларига йўл қўймаслик учун, тармоқларда маршрутлашни, компьютер уланишларини ҳамда ахборот оқимларини бошқариш воситаларини жорий этиш керак**.**

Жорий этиш бўйича қўлланма

Маршрутлашни бошқариш воситалари жўнатувчи ва олувчининг белгиланган адресларини текшириш мезханизмига асосланган бўлиши керак.

Агар Proxy ва/ёки тармоқ адресларини трансляция қилиш технологияларидан фойдаланилса, жўнатувчи ва олувчининг ҳақиқий адресларини текшириш учун ички ва ташқи тармоқларнинг назорат нуқталарида хавфсизлик шлюзларидан фойдаланса бўлади. Жорий этиш билан шуғулланадиган мутахассислар фойдаланилаётган технологиянинг тавсифлари тўғрисида хабардор бўлишлари зарур.

Тармоқли маршрутлашни бошқаришга қўйилган талабларни фойдаланишни бошқариш сиёсатида асослаш керак (11.1).

Бошқалар

Биргаликда фойдаланиладиган тармоқларда, айниқса ташкилот ташқарисига чиқадиганларида, қўшимча маршрутлашни бошқариш воситалари зарур бўлиши мумкин. Бу айниқса учинчи томон (ташкилот ходимлари ҳисобланмайдиган) фойдаланувчилари томонидан фойдаланиладиган тармоқларда қўлланади.

11.5 Операцион тизимлардан фойдаланишни бошқариш

Мақсад: операцион тизимлардан рухсатсиз фойдаланишнинг олдини олиш.

Авторизация қилинган фойдаланувчиларнинг фойдаланишини чеклаш учун операцион тизим даражасида ахборот хавфсизлиги воситаларини ишлатиш керак. Бу воситалар қуйидагиларни таъминлаши керак:

a) авторизация қилинган фойдаланувчиларни фойдаланишни бошқаришнинг белгиланган сиёсатига мувофиқ аутентификация қилиш;

b) тизимдан муваффақиятли ва муваффақиятсиз фойдаланишга уринишни рўйхатга олиш;

c) махсус тизим имтиёзларидан фойдаланишни рўйхатга олиш;

d) тизим хавфсизлигининг сиёсатлари бузилганда авария тўғрисида хабар бериш;

e) тегишли даражани аутентификация қилиш;

f) зарур бўлган ҳолда фойдаланувчиларнинг уланиш вақтини чеклаш.

11.5.1 Тизимга хавфсиз кириш тартиби

Бошқариш воситаси

Ахборот сервисларидан фойдаланиш тизимга хавфсиз кириш процедурасидан фойдаланиш ёрдамида таъминланган бўлиши керак.

Жорий этиш бўйича қўлланма

Компьютер тизимида рўйхатга олиш процедурасини шундай лойиҳалаштириш керакки, рухсатсиз фойдаланиш имконияти минимумга

келтирилсин ва авторизация қилинмаган фойдаланувчига ёрдам берилмасин. Тўғри режалаштирилган рўйхатга олиш процедураси қуйидаги хусусиятларга эга бўлиши керак:

a) рўйхатга олиш жараёни муваффақиятли тугатилмагунича тизимлар ёки иловалар номларини акс эттирмаслик;

b) компьютердан фақат авторизация қилинган фойдаланувчилар фойдаланиши мумкинлиги тўғрисида огоҳлантирувчи умумий хабарномани акс эттириш;

c) рўйхатга олиш процедураси давомида авторизация қилинмаган фойдаланувчиларга ёрдам бериши мумкин бўлган хабарлар - йўл-йўриқларни тақдим этмаслик;

d) рўйхатга олиш ахборотини фақат барча кириш маълумотлари киритилганидан сўнг тасдиқлаш. Хато киритилган ҳолатда маълумотларнинг қайси қисми тўғри ёки нотўғрилигини тизим кўрсатмаслиги керак;

e) рухсат берилган муваффақиятсиз уринишлар сонини чеклаш ва қуйидагиларни кўзда тутиш:

1) муваффақиятсиз ва муваффақиятли уринишларни рўйхатга олиш;

2) рўйхатга олишнинг кейинги уринишлари ўртасидаги вақтинчалик кечикишни улаш ёки исталган махсус авторизациясиз рўйхатга олишнинг кейинги уринишларини рад этиш;

3) маълумотларни узатишда алоқа сеансини узиш;

4) агар тизимга киришга уринишларнинг максимал сонига эришилган бўлса, сигналли хабарларни тизим консолига йўналтириш;

5) паролга киришга қайта уринишлар сонини паролнинг минимал узунлигига ва муҳофаза қилинаётган тизимнинг қийматига мувофиқ белгилаш;

f) рўйхатга олиш процедураси учун рухсат берилган максимал ва минимал вақтни чеклаш. Агар у кўпайтирилган бўлса, тизим рўйхатга олишни тўхтатиши керак;

g) муваффақиятли тугатилган рўйхатга олишга тегишли ахборотни қайд қилиш;

1) аввалги муваффақиятли рўйхатга олиш санаси ва вақтини;

2) охирги муваффақиятли рўйхатга олишдан бошлаб, ҳар қандай муваффақиятсиз рўйхатга олишга уринишлар деталларини;

h) киритилаётган паролни кўрсатмаслик ёки вариант сифатида пароль белгиларини символлар билан беркитиш;

i) парольларни оддий матнда тармоқ орқали узатмаслик.

Бошқалар

Агар пароллар тизимга кириш сеанси жараёнида тармоқ орқали оддий матнда узатилса, улар тармоқда «сниффером» дастури орқали тутиб олиниши мумкин.

11.5.2 Фойдаланувчиларни идентификация ва аутентификация қилиш

Бошқариш воситаси

Ҳар бир фойдаланувчида фақат якка фойдаланиш учун фойдаланувчининг ноёб идентификатори бўлиши керак (ID фойдаланувчисининг идентификатори), фойдаланувчининг шахсини тасдиқлаш учун эса, аутентификация қилишнинг мақбул методи танланиши керак.

Жорий этиш бўйича қўлланма

Ушбу бошқариш воситасини фойдаланувчилар (жумладан техник таъминот ходимлари, операторлар, тармоқ маъмурлари, тизим дастурчилари ва маълумотлар базаси маъмурлари)нинг барча турлари учун қўллаш керак.

Фойдаланувчилар идентификаторларини жавобгар шахс томонидан хатти-ҳаракатларни кузатиш учун қўллаш керак. Фойдаланувчиларнинг кундалик хатти-ҳаракатларини имтиёзли ҳисобга олиш ёзувлари остида бажариш мумкин эмас.

Ўта муҳим ишларни ёки муайян ишни бажариш учун фойдаланувчиларнинг гуруҳи учун умумий идентификатордан фойдаланишга йўл қўйилади. Бундай ҳолларда тегишли тарзда раҳбариятнинг рухсатномаси расмийлаштирилиши керак. Бундан ташқари, рухсатсиз фойдаланишдан тизим хавфсизлигини таъминлаш учун, бундай ҳолларда ахборот хавфсизлигини таъминлашнинг қўшимча чораларини қўллаш талаб қилиниши мумкин.

Шахсий фойдаланиш учун умумий фойдаланиш идентификаторларидан фойдаланишга бундай идентификаторнинг фойдаланувчилари томонидан бажариладиган фойдаланиш функциялари ёки амалларини кузатиб бориш (масалан, фойдаланиш фақат ўқиш учун) керак бўлмаса, ёки бошқаришнинг бошқа воситалари (масалан, умумий идентификатор учун пароль бир марта фақат ходимларнинг бир гуруҳига берилади ва ушбу ҳодиса рўйхатга олинади) бўлса, рухсат бериш керак.

Аутентификация ва идентификация қилиш учун, шунингдек, паролларни аутентификация қилишнинг криптографик воситалари, микропроцессорли карталари (смарт карталар) каби, фойдаланишнинг махсус физик хотирали (токенлар) қурилмаларидан ёки аутентификация қилишнинг биометрик методлари каби муқобил методларидан фойдаланиш мумкин.

Бошқалар

Пароллар (11.3.1, 11.5.3) - идентификация ва аутентификация қилишни таъминлашнинг фақат фойдаланувчига маълум бўлган сирга асосланган умум қабул қилинган усули. Ўшанинг ўзига криптография воситалари ва аутентификация қилиш баённомалари орқали эришиш мумкин. Фойдаланувчиларни идентификация ва аутентификация қилишнинг барқарорлиги фойдаланиш амалга оширилаётган ахборот конфиденциаллигига мувофиқ бўлиши керак.

Шунингдек, идентификация ва аутентификация қилиш учун фойдаланувчилар эгалик қилган токенлар ёки смарт-карталар каби предметлардан фойдаланиш мумкин. Инсон шахсини аутентификация қилиш учун, шунингдек, аутентификация қилишнинг инсоннинг ноёб тавсифлари ёки белгиларидан фойдаланувчи биометрик технологиялари қўлланиши мумкин. Ишончли боғланган технологиялар ва механизмларни бирлаштириш янада барқарорроқ аутентификация қилишга олиб келади.

11.5.3 Паролларни бошқариш тизими

Бошқариш воситаси

Паролларни бошқариш тизимлари интерактив ва сифатли паролларни кафолатловчи бўлиши керак.

Жорий этиш бўйича қўлланма

Паролларни бошқариш тизими қуйидагиларни амалга ошириши керак:

a) жавобгарликни белгилаш учун фойдаланувчиларнинг индивидуал идентификаторлари ва паролларидан фойдаланишни таъминлаш;

b) фойдаланувчиларга ўзларининг индивидуал паролларини танлаш ва ўзгартиришга, шунингдек, киритиш хатолари бўлганда уларни тасдиқлаш тартибини киритишга рухсат бериш;

c) сифатли паролларни танлашни таъминлаш (11.3.1);

d) паролларни ўзгартиришни таъминлаш (11.3.1);

e) биринчи бор рўйхатдан ўтказишда вақтинчалик паролларни ўзгартиришни таъминлаш (11.2.3);

f) фойдаланувчиларнинг аввалги паролларини сақлашни таъминлаш ва улардан қайта фойдаланишнинг олдини олиш;

g) паролларни киритишда уларни экранда акс эттирмаслик;

h) пароллар файлларини амалий тизимлар маълумотларидан алоҳида сақлаш;

i) паролларни (масалан, шифрланган ёки хешифрланган) муҳофаза қилинган шаклда сақлаш ва узатиш;

Бошқалар

Пароллар - компьютер сервисларидан фойдаланаётган фойдаланувчининг ваколатларини тасдиқлайдиган асосий воситалардан биридир.

Баъзи бизнес-иловалар учун фойдаланувчилар паролларини алоқаси бўлмаган мансабдор шахс томонидан белгилаш талаб қилинади; бундай ҳолларда юқорида эсга олинган қўлланманинг b, d ва e бандлари қўлланмайди. Кўп ҳолларда пароллар фойдаланувчилар томонидан танланади ва сақлаб турилади (11.3.1).

11.5.4 Тизим утилитларидан фойдаланиш

Бошқариш воситаси

Тизимли ва амалий бошқарш воситаларини бостириш қобилиятига эга дастурий утилитлардан фойдаланишни чеклаш ва қатъий бошқариш керак.

Жорий этиш бўйича қўлланма

Тизим утилитларидан фойдаланиш бўйича қуйидаги тавсияларни бажариш зарур:

a) тизим утилитлари учун идентификация қилиш, аутентификация қилиш ва рухсат бериш процедураларидан фойдаланиш;

b) тизим утилитлари ва амалий дастурий таъминотни ажратиш;

c) тизим утилитларидан фойдаланиш зарурати бўлган авторизация қилинган фойдаланувчиларнинг минимал сонини танлаш йўли билан чеклаш (11.2.2);

d) ҳар бир муайян ҳодиса учун тизим утилитларидан фойдаланишга рухсат бериш;

e) тизим утилитларидан фойдаланишни чеклаш, масалан, фақат авторизация қилинган ўзгаришлар киритиш пайтида;

f) барча тизим утилитларидан фойдаланишни рўйхатга олиш;

g) тизим утилитларига тегишли авторизация қилиш даражаларини белгилаш ва ҳужжатлаштириш;

h) тизим дастурий таъминотидан барча кераксиз утилитларни чиқариб ташлаш;

i) мажбуриятлар тақсимланиши зарур бўлган тизимлардаги иловалардан фойдаланиш ҳуқуқига эга бўлган фойдаланувчиларга тизим утилитларидан фойдаланишга йўл қўймаслик.

Бошқалар

Кўпгина компьютерларда утилитнинг операцион тизимлар ва бизнес-иловалардан рухсатсиз фойдаланишнинг олдини олиш чораларини айланиб ўтишга имкон берадиган, ҳеч бўлмаганда, битта тизим сервис дастури ўрнатилади.

11.5.5 Сеансда танаффус

Бошқариш воситаси

Амалда бўлмаган терминаллар маълум вақт бекор турганидан сўнг ўчиши керак.

Жорий этиш бўйича қўлланма

Вақт бўйича блокировкалаш механизми терминал экранини тозалашни, шунингдек, терминал маълум бир вақт амалда бўлмаган даврдан сўнг унинг илова сеансларининг ишини ва терминал тармоқ сеансини беркитишни таъминлаши керак. Блокировканинг ишга тушиш вақти терминални ўрнатиш жойи, ишлов бериладиган ахборотнинг ва фойдаланиладиган иловаларнинг таснифи, шунингдек, фойдаланувчилар билан боғлиқ хавфлар ҳисобга олиниб белгиланиши керак.

Шуни назарда тутиш керакки, баъзи шахсий компьютерлар иловалар ёки тармоқ сеансини беркитмасдан экранни тозалаш ва рухсатсиз фойдаланишнинг олдини олиш йўли билан терминални вақт бўйича блокировкалашнинг чекланган имкониятини таъминлайди.

Бошқалар

Бошқаришнинг ушбу воситаси айниқса ташкилот хавфсизлигини бошқариш ва назорат қилиш зонасидан ташқаридаги ҳамма эркин фойдаланиши мумкин бўлган ёки ташқи участкаларни ўз ичига оладиган катта хавфга эга бўлган жойларда жуда муҳим. Сеанслар авторизация қилинмаган шахсларнинг фойдаланишини ва «хизмат кўрсатишдан бош тортиш» каби ҳужумларнинг олдини олиш учун тугатилиши керак.

11.5.6 Уланиш вақтини чеклаш

Бошқариш воситаси

Уланиш вақтини чеклаш катта хавфга эга бўлган иловалар учун қўшимча хавфсизликни таъминлаши керак.

Жорий этиш бўйича қўлланма

Уланиш вақтини чеклаш чорасини энг конфиденциал компьютер иловалари учун қўллаш керак, айниқса, катта хавфга эга бўлган жойларда, масалан ҳамма эркин фойдаланиши мумкин бўлган жойларда ёки ташкилот хавфсизлигини бошқаришни назорат қилиш соҳасидан ташқарида ўрнатилган терминаллар билан боғлиқ бўлган иловалар учун. Бундай чеклашларга мисоллар:

a) файлларни ёки узоқ давом этмайдиган мунтазам интерактив сеансларни пакетли узатиш учун олдиндан белгиланган вақт оралиғидан фойдаланиш;

b) агар ишдан ташқари ишлашга ёки кўпроқ чўзиладиган ишга зарурат бўлмаса, ташкилот ишининг соатлаб уланиш вақтини чеклаш.

c) режалаштирилган вақт оралиғидан сўнг такроран аутентификация қилишни кўриб чиқиш.

Бошқалар

Терминалларни компьютер сервисларига уланиш учун рухсат берилган вақт орлиғини чеклаш рухсат берилмаган фойдаланиш имкони бўлган вақт оралиғини камайтиради. Актив сеансларнинг давомийлигини чеклаш қайта аутентификация қилишни хоҳламаган фойдаланувчилар томонидан очиқ сеанслар сақланиб туришига халақит қилади.

11.6 Иловалар ва ахборотдан фойдаланишни бошқариш

Мақсад: амалий тизимлардаги ахборотлардан рухсатсиз фойдаланишнинг олдини олиш.

Амалий тизимлар ва уларнинг ичидаги ахборотдан фойдаланишни чеклаш учун хавфсизлик воситаларидан фойдаланиш керак.

Дастурий таъминот ва ахборотдан мантиқий фойдаланиш фақат авторизация қилинган фойдаланувчиларга тақдим этилиши керак. Бунинг учун қуйидагиларни таъминлаш зарур:

a) фойдаланишни бошқариш сиёсатига мувофиқ фойдаланувчиларнинг ахборот ва бизнес-иловалар функцияларидан фойдаланишини бошқариш;

b) операцион тизим ёки иловаларнинг назорат механизмларини четлаб ўтишга имкон берадиган ҳар қандай утилитлардан ва тизим дастурий таъминотидан рухсатсиз фойдаланишдан муҳофаза қилиш;

c) ахборот активлари биргаликда фойдаланадиган бошқа тизимлар хавфсизлигини компрометация қилинишининг олдини олиш.

11.6.1 Ахборотдан фойдаланишни чеклаш

Бошқариш воситаси

Ахборотдан ва фойдаланувчилар ҳамда ёрдамчи ходимларнинг амалий тизим функцияларидан фойдаланишини фойдаланишни бошқаришнинг муайян сиёсатига мувофиқ чеклаш керак.

Жорий этиш бўйича қўлланма

Фойдаланишни чеклаш алоҳида бизнес-иловаларга қўйилган шахсий талабларга асосланиши керак. Шунингдек, фойдаланишни бошқариш сиёсати, ташкилотнинг фойдаланиш сиёсатига қарши бўлмаслиги керак (11.1).

Фойдаланишни чеклаш бўйича талабларни қондириш учун қуйидаги тадбирларнинг қўлланишини кўриб чиқиш зарур:

a) тизимнинг амалий функцияларидан фойдаланшни бошқариш учун менюни сақлаш;

b) фойдаланувчиларнинг фойдаланиш ҳуқуқини назорат қилиш, масалан, ўқиш, ёзиб олиш, йўқ қилиш, бажариш;

c) бошқа иловаларнинг фойдаланиш ҳуқуқларини бошқариш;

d) конфиденциал ахборотга ишлов берадиган бизнес-иловалардан чиқариладиган маълумотлар талаб қилинган ахборотга эгаликларига ва фақат авторизация қилинган терминалларнинг адресига ва тайинланган жойга юборилишига ишонч ҳосил қилиш. Ортиқча ахборотни йўқ қилиш учун чиқариш жараёнини даврий равишда таҳлил қилиб туриш керак.

11.6.2 Конфиденциал ахборотга ишлов берадиган тизимларни ажратиш

Бошқариш воситаси

Конфиденциал ахборотга ишлов берадиган тизимлар ажратилган (изоляцияланган) ҳисоблаш муҳити билан таъминланган бўлиши керак.

Жорий этиш бўйича қўлланма

Конфиденциал ахборотга ишлов берадиган тизимларни ажратиш учун қуйидаги бандларни кўриб чиқиш зарур:

a) бизнес-иловалар (7.1.2) эгаси уларнинг конфиденциаллик даражасини аниқлаши ва ҳужжат билан расмийлаштириши зарур;

b) конфиденциал бизнес-илова биргаликда фойдаланиш муҳитида ишлаши керак бўлса, активлардан биргаликда фойдаланиш амалга оширилиши керак бўлган бошқа иловаларни аниқлаш ва буни конфиденциал бизнес-илова эгаси билан келишиш керак.

Бошқалар

Баъзи амалий тизимлар маълумотлар хавфсизлиги нуқтаи назаридан жуда сезгир ҳисобланади ва шунинг учун эксплуатация қилишнинг махсус шароитларини талаб қиладилар. Ишлов бериладиган ахборотнинг конфиденциаллик даражаси қуйидагиларни талаб қилиши мумкин:

a) ажратилган компьютерда ишлаш;

b) активлардан фақат хавфсиз бизнес-иловалар билан биргаликда фойдаланиш ёки ҳеч қандай чеклашларсиз ишлаш.

Ажратишни жисмоний ва мантиқий методлардан фойдаланиб таъминлаш мумкин (11.4.5).

11.7 Мобил компьютерлар билан масофадаги режимда ишлаш

Мақсад: мобил компьютерлардан ва масофадаги режимда ишлашни таъминловчи воситалардан фойдаланишда ахборот хавфсизлигини таъминлаш.

Талаб қилинган муҳофазани масофадаги режимда ишлашнинг ўзига хос хавфлари билан солиштириш керак. Мобил компьютерлардан фойдаланишда муҳофазаланмаган муҳитда ишлаш билан боғлиқ хавфлар ҳисобга олиниши ва муҳофаза қилишнинг тегишли чоралари кўрилиши керак. Масофадаги режимда ишлаган ҳолларда ташкилот иш жойининг муҳофазасини ва ахборот хавфсизлигини таъминлаш бўйича тегишли чораларни назарда тутиши керак.

11.7.1 Мобил компьютерлар ва телекоммуникация воситалари

Бошқариш воситаси

Мобил компьютерлар ва телекоммуникация воситаларидан фойдаланиш билан боғлиқ хавфлардан муҳофаза қилиш учун расмий сиёсатни жорий этиш ва хавфсизликнинг тегишли чораларини кўриш керак.

Жорий этиш бўйича қўлланма

Мобил ҳисоблаш қурилмалари ва телекоммуникация воситаларидан, масалан, ноутбуклар, чўнтак компьютерлари, лэптоплар, смартфонлар ва мобил телефонлардан фойдаланишда хизматга оид ахборотни компрометация қилишнинг олдини олиш учун ўта эҳтиёткорликка риоя қилиш керак. Мобил қурилмалардан фойдаланиш сиёсати, айниқса, муҳофазаланмаган муҳитда, мобил қурилмалар билан ишлашда боғлиқ хавфларни ҳисобга олиши керак.

Мобил қурилмалардан фойдаланиш сиёсати жисмоний муҳофаза бўйича, фойдаланишни бошқариш, криптография воситалари ва методларидан фойдаланиш, шунингдек, резервлаш ва вируслардан муҳофаза қилиш бўйича талабларни ўз ичига олиши керак. Ушбу сиёсат мобил қурилмаларни тармоққа улаш, шунингдек, улардан умумжамоат жойларида фойдаланиш бўйича қўлланмани ишлаб чиқиш бўйича қоида ва тавсияларни ўз ичига олиши зарур.

Умумжамоат жойларида, сўзлашув хоналарида ва ташкилотдан ташқаридаги муҳофазаланмаган хоналарда мобил қурилмалардан фойдаланишда эҳтиёткорликка риоя қилиш керак. Мобил қурилмалардан рухсатсиз фойдаланиш ёки ушбу қурилмалар ёрдамида сақланадиган ва ишлов бериладиган ахборотни, масалан, криптографик методлардан фойдаланган ҳолда, ошкор қилишнинг олдини олиш мақсадида, муҳофаза қилишни жорий этиш керак (12.3).

Умумжамоат жойларида мобил қурилмалардан фойдаланишда бегона шахслар томонидан билдирмасдан кўриб олиш хавфини камайтириш учун эҳтиёткорлик билан иш тутиш муҳим. Зарар келтирувчи дастурий таъминотдан муҳофаза қилиш воситалари ва усулларини актуализация қилинган ҳолатда жорий қилиш ва сақлаб туриш зарур (10.4).

Конфиденциал ва сезгир хизматга оид ахборотнинг резерв нусхаларини мунтазам яратиб туриш керак. Ахборотни тезроқ ва қулай резервлаш имкониятига эга бўлиш учун ускунадан фойдалана олиш керак. Ушбу резерв нусхаларни ўғирлашдан ёки ахборотни йўқотишдан тегишли тарзда муҳофаза қилиш керак.

Умумий фойдаланиш тармоғига уланган мобил қурилмаларнинг тегишли муҳофазасини қўллаш керак. Мобил воситалардан фойдаланиб, умумий фойдаланиш тармоғи орқали конфиденциал ахборотдан узоқдан туриб фойдаланишга фақат муваффақиятли идентификация ва аутентификация қилишдан сўнг, шунингдек, фойдаланишни бошқаришнинг тегишли механизмлари мавжудлигида йўл қўйилади (11.4).

Мобил қурилмаларни, шунингдек, ўғирликдан жисмоний муҳофаза қилиш керак, уларни қаровсиз қолдириш тавсия этилмайди, масалан автомобиллар ёки транспортнинг бошқа турларида, меҳмонхоналарда ва конференц-залларда.

Мобил қурилмалари ўғирланган ёки йўқотилган ҳоллар учун ташкилотнинг юридик, суғуртага оид ва бошқа хавфсизлик талабларини эътиборга олувчи алоҳида қоидаларни тасдиқлаш керак. Конфиденциал, ёпиқ ва/ёки хизматга оид сезгир ахборотга эга бўлган ускунани қаровсиз қолдириш мумкин эмас ва имкони борича уларни ишончли жойга жисмонан беркитиш ёхуд ускунани муҳофаза қилиш учун махсус қулфлардан фойдаланиш керак (9.2.5).

Мобил компьютерлардан фойдаланадиган ходимларни қўшимча хавфлар ва ишлашнинг ушбу усули билан боғлиқ ахборот хавфсизлигини таъминлашнинг зарур тадбирлари тўғрисида хабардор қилиш зарур.

Бошқалар

Симсиз мобил уланишлар тармоқ уланишларининг бошқа турларига ўхшаш, лекин бошқариш воситасини белгилашда кўриб чиқилиши керак бўлган муҳим фарқларга эга. Аниқ кўриниб турган фарқлар*:*

a) баъзи симсиз хавфсизлик протоколлари мукаммал эмас деб ҳисобланади ва заифликларга эга;

b) мобил компьютерларда сақланадиган ахборот тармоқнинг ўтказиш полосаси чекланганлиги туфайли ва/ёки мобил ускунанинг резервлаш учун мўлжалланган вақтда уланмаганлиги учун резервланмаслиги мумкин.

11.7.2 Масофадаги режимда ишлаш

Бошқариш воситаси

Масофадаги режимда ишлаш сиёсатини, ишга оид режаларни ва ишлаш тартибини ишлаб чиқиш ва жорий этиш керак.

Жорий этиш бўйича қўлланма

Ташкилотлар масофадаги режимда ишлаш имкониятини ахборот хавфсизлигининг ташкилот хавфсизлиги сиёсатига мос келадиган тегишли чоралари қўлланишига ишонч ҳосил қилганларидагина авторизация қилишлари керак.

Масофадаги иш жойини ускуна ва ахборотларни ўғирлашдан, ахборотни рухсатсиз ошкор қилишдан, ташкилотнинг ички тизимларидан узоқлаштирилган рухсатсиз фойдаланиш ёки ускунадан нотўғри фойдаланишдан муҳофаза қилинишини таъминлаш зарур. Масофадаги режимда ишлашда авторизация қилиш талаблари каби раҳбарлар томонидан назорат қилиш бўйича талаблар ҳам бажарилган бўлиши, шунингдек, ушбу иш усулининг тегишли ахборот хавфсизлик даражаси таъминланган бўлиши муҳим.

Қуйидагиларни эътиборга олиш зарур:

a) бино ва атроф-муҳитнинг хавфсизлиги нуқтаи назаридан масофадаги режимдаги иш жойининг мавжуд жисмоний хавфсизлиги;

b) масофадаги иш жойларининг тавсия этиладиган ускунаси;

c) ташкилотнинг ички тизимларидан ва фойдаланиш амалга ошириладиган ва телекоммуникация каналлари бўйлаб узатиладиган конфиденциал ахборотдан узоқлаштирилган фойдаланишга бўлган эҳтиёждан келиб чиқиб, коммуникация хавфсизлигига қўйилган талаблар, шунингдек, ташкилот ички тизимларининг конфиденциаллиги;

d) масофадаги иш жойларидан фойдаланиш ҳуқуқига эга бўлган бошқа шахслар, масалан, оила аъзолари ва дўстлари томонидан ахборотлар ёки активлардан рухсатсиз фойдаланиш таҳдиди;

e) уй тармоқларидан фойдаланиш, шунингдек, симсиз тармоқлар сервислари конфигурациясига талаблар ёки чеклашлар;

f) хусусий мулк эгалигида бўлган ускунада яратилган интеллектуал мулкка эгалик ҳуқуқлари тўғрисидаги бахсларнинг олдини олиш сиёсати ва тартиби;

g) қонун ҳужжатлари томонидан ман этилиши мумкин бўлган (хавфсизликни текшириш учун ёки текширув вақтида) хусусий мулк эгалигида бўлган ускунадан фойдаланиш;

h) дастурий таъминот учун лицензион контрактлар мавжуд бўлганда ташкилотлар ходимлар, субпудратчилар ёки бегона ташкилотлар фойдаланувчилари ўзларининг ишлаш станцияларининг мижозлар дастурий таъминотини лицензиялаш учун жавобгар бўлиши мумкин;

i) вирусга қарши муҳофаза ва тармоқлараро экранга қўйилган талаблар.

Кўриб чиқилиши керак бўлган тавсиялар ва тадбирлар қуйидагиларни ўз ичига олади:

a) ўзининг ускунасидан фойдаланишга рухсат берилмаган масофадаги иш жойларини тўғри келадиган ускуна ва мебель билан таъминлаш;

b) рухсат берилган иш турларини, иш вақтини, сақланиши мумкин бўлган ахборот таснифини белгилаш, шунингдек, масофадаги режимда ишлайдиган шахсга фойдаланиш рухсат берилган ички тизимлар ва хизматларни белгилаш;

c) тўғри келадиган телекоммуникация ускунаси билан таъминлаш, жумладан узоқдаги фойдаланишнинг хавфсизлигини таъминлаш воситалари билан;

d) жисмоний хавфсизлик;

e) ускуна ва ахборотдан оила аъзолари ва дўстларнинг фойдаланишига тегишли қоида ва қўлланмалар;

f) ускуна ва дастурий таъминотни сақлаб туриш ва унга хизмат кўрсатишни таъминлаш;

g) суғурталашни таъминлаш;

h) маълумотларни резервлаш ва фаолиятнинг узлуксизлигини таъминлаш процедуралари;

i) хавфсизлик аудити ва мониторинги;

j) масофадаги режимда иш тўхтаган ҳолда ваколатларини, фойдаланиш ҳуқуқларини бекор қилиш ва ускунани қайтариш.

Бошқалар

Масофадаги режимда ишлашда, шунингдек, ходимларнинг ўз ташкилотидан ташқарида ишлашини таъминлаш учун муайян узоқдаги жойда инфокоммуникацион технологиялардан фойдаланилади.

12 Ахборот тизимларини сотиб олиш, ишлаб чиқиш ва уларга хизмат кўрсатиш

12.1 Ахборот тизимларининг хавфсизлигига қўйиладиган талаблар

Мақсад: хавфсизликни таъминлаш ахборот тизимларининг ажралмас қисмидир.

Ахборот тизимлари операцион тизимларни, инфратузилмани, бизнес иловаларни, тайёр маҳсулотлар, сервислар ва фойдаланувчилар томонидан ишлаб чиқилган иловаларни ўз ичига олади. Лойиҳалаш ва бизнес-илова ёки сервисни жорий қилиш жараёнлари хавфсизлик нуқтаи назаридан сезгир бўлиши мумкин. Хавфсизлик талаблари ахборот тизимларини ишлаб чиқишга қадар белгиланган ва келишилган бўлиши керак.

Хавфсизликнинг барча талабларини ахборот тизимининг техник топшириғини ишлаб чиқиш босқичида белгилаш керак. Улар умумий лойиҳа доирасида белгиланган, асосланган, келишилган ва ҳужжатлаштирилган бўлиши керак.

12.1.1 Хавфсизлик талабларини таҳлил қилиш ва спецификациялаш

Бошқариш воситаси

Янги тизимларга ёки мавжуд тизимларни модернизация қилишга нисбатан бизнес талабларининг ифодаларида ахборот хавфсизлиги талаблари ҳисобга олинган бўлиши зарур.

Жорий этиш бўйича қўлланма

Тизимга ўрнатилган бошқариш автоматик воситаларининг имкониятларини ҳисобга олиш зарур, шунингдек, хавфсизликни бошқаришнинг ёрдамчи дастаки воситаларидан фойдаланиш имкониятини ҳам кўриб чиқиш керак. Амалий дастурларнинг пакетларини баҳолашга ҳам худди шундай ёндашиш керак.

Тизим хавфсизлигига ва уни бошқариш воситаларига қўйилган талаблар ахборот активларининг аҳамиятини (7.2), хавфсизлик чораларининг самарасизлиги ёки йўқлиги натижасида бизнесга етказилиши мумкин бўлган потенциал зарарни ҳисобга олиши керак.

Ахборот хавфсизлигининг тизим талабларини ва хавфсизликни жорий қилиш жараёнлари ахборот тизимлари лойиҳаларининг дастлабки босқичларида бирлаштирилиши керак. Тизимни лойиҳалаш бос-қичида унинг хавфсизлигига қўйилган талабларни амалга ошириш тизимни жорий қилиш вақтида ёки ундан сўнг тегишли воситаларни ишлаб чиқишга қараганда кетадиган сарф-харажатларни сезиларли даражада пасайтириш имконини беради.

Агар маҳсулот сотиб олинадиган бўлса, расмий синаш ва сотиб олиш жараёнига риоя қилиш керак. Етказиб берувчилар билан тузиладиган

шартномалар хавфсизликнинг белгиланган талабларини ҳисобга олиши керак. Агар хавфсизликнинг функционал имкониятлари таклиф этилган маҳсулотда белгиланган талабларга жавоб бермаса, олиб кирилаётган хавф ва у билан боғлиқ бўлган бошқариш воситаларини маҳсулот сотиб олингунга қадар қайта кўриб чиқиш керак. Агар хавф-сизлик хавфларини чақирувчи қўшимча функционал имкониятлар берилса, уларни ўчириб қўйиш ёки фойдаланиш мумкин бўлган қўшимча функционал имкониятлардан фойда олиш мумкинлигини аниқлаш учун таклиф этилган бошқариш структурасини қайта кўриб чиқиш керак.

Бошқалар

Раҳбарият, масалан, нархини ҳисобга олиб мустақил баҳога ва сертификатга эга бўлган маҳсулотлардан фойдаланишни жоиз деб топиши мумкин. Бундан кейинги АТ хавфсизлик маҳсулотлари баҳосининг мезон-лари тўғрисидаги ахборот O‘z DSt ISO/IEC 15408:2008 стандартида ёки, зарурат бўлганда баҳолаш ва сертификатлашнинг бошқа стандартларида бўлади.

ISO/IEC 13335-3 стандарти хавфсизликни бошқариш воситаларига қўйилган талабларни белгилаш учун хавфларни бошқариш жараёнларидан фойдаланиш бўйича қўлланмани ўз ичига олади.

12.2 Иловаларда ахборотга тўғри ишлов бериш

Мақсад: иловаларда хатолар, йўқотишлар, рухсатсиз модификация қилиш ёки ахборотдан ғайриқонуний фойдаланишларнинг олдини олиш.

Амалий тизимларда, жумладан фойдаланувчиларнинг ўзлари томонидан ёзилган иловаларда ахборот хавфсизлигини таъминлаш бўйича тегишли тадбирларни, шунингдек, аудит ёки фойдаланувчи хатти-ҳаракатларининг баённомасини тузишни кўзда тутиш зарур. Улар ўз ичига кирувчи, оралиқ ва чиқувчи маълумотларни текшириш функцияларини олиши керак.

Ахборот хавфсизлигини таъминлаш бўйича қўшимча тадбирлар ташкилотнинг конфиденциал, қимматли ёки критик активларига ишлов берадиган ёки таъсирини ўтказадиган тизимлар учун талаб қилиниши мумкин ва уларни хавфсизлик ва хавфларни баҳолаш талаблари асосида аниқлаш зарур.

12.2.1 Кирувчи маълумотлар тўғрилигини тасдиқлаш

Бошқариш воситаси

Иловалар кирувчи маълумотларининг тўғрилиги ва яроқлилиги текширилиши керак.

Жорий этиш бўйича қўлланма

Бизнес-транзакциялар, доимий маълумотлар (мижозларнинг номлари ва манзиллари, кредит лимитлари, идентификация қилиш рақамлари)и ва параметрлар жадваллари (сотиш нархлари, валюталар курслари, солиқлар ставкалари)ни киритишда кирувчи маълумотларнинг бошланғич маълумотларга мувофиқлигига ишонч ҳосил қилиш учун

уларнинг тўғрилиги текширилади. Бунинг учун қуйидаги тадбирларни кўриб чиқиш мақсадга мувофиқ:

а) икки баравар кўп киритиш ёки қуйидаги хатоларни аниқлаш мақсадида чегараларни текшириш ёки киритиш майдонларини кирувчи маълумотларнинг муайян диапазонлари билан чеклаш каби киритиладиган маълумотларнинг бошқа текширувлари:

1) рухсат берилган диапазондан чиқадиган қийматлар;

2) маълумотлар майдонида йўл қўйиб бўлмайдиган символлар;

3) мажуд бўлмаган ёки тўлиқ бўлмаган маълумотлар;

4) маълумотлар ҳажмининг юқори ва қуйи чегараларидан ошиб кетиши;

5) рухсат берилмаган ёки бошқарувга зид маълумотлар;

b) асосий майдонлар ёки маълумотлар файллари таркибининг ишончлилиги ва бутлигини тасдиқлаш учун даврий равишда таҳлил қилиш (кўздан кечириш);

c) маълумотларнинг ҳар қандай рухсат берилмаган ўзгаришларини аниқлаш учун киритилаётган ҳужжатларнинг ўзгармас (босиб чиқарилган) нусхаларини киритилаётган маълумотлар билан солиштириш (ҳужжатлардаги барча ўзгаришларга рухсат берилган бўлиши зарур);

d) маълумотларнинг тўғрилигини тасдиқлаш билан боғлиқ хатоларга муносабат билдириш тартиби;

e) киритилаётган маълумотларнинг тўғрилигини текшириш тартиби;

f) маълумотларни киритиш жараёнида қатнашадиган барча ходимларнинг мажбуриятларини белгилаш;

g) маълумотларни киритиш жараёнида бажариладиган амалларни рўйхатга олиш журналини юритиш (10.10.1).

Бошқалар

Хатолар хавфини камайтириш ва стандарт ҳужумларнинг, жумладан буфернинг тўлиб кетиши ва кодни киритишнинг олдини олиш мақсадида қўлласа бўладиган жойда автоматик таҳлил ва кирувчи маълумотларнинг тўғрилигини текширишни кўриб чиқиш мумкин.

12.2.2 Иловаларда маълумотларга ишлов беришни бошқариш

Бошқариш воситаси

Ишлов бериш хатолари ёки атайлаб қилинган хатти-ҳаракатлар туфайли ахборотнинг бузилишини аниқлаш учун иловаларда тўғриликни текшириш керак.

Жорий этиш бўйича қўлланма

Иловаларнинг архитектураси маълумотлар бутлигини йўқотишга олиб келадиган, инкор қилиш хавфини минимумга келтиришга қаратилган чеклашлар амалга оширилганлигига ишончни таъминлаши керак. Хусусан, қуйидагилар ҳисобга олиниши керак:

a) дастурларда маълумотлар ўзгаришларини келтириб чиқарадиган қўшиш ва йўқ қилиш функцияларидан фойдаланиш ва уларни жойлаштириш;

b) ишга нотўғри тушириш ёки маълумотларга ишлов беришдан олдин тўхтаб қолишдан сўнг дастурнинг нотўғри ишини олдини оладиган процедуралар (8.1.1);

c) тўхтаб қолишдан сўнг тиклаш ва маълумотларга тўғри ишлов берилишини таъминлаш учун тузатувчи дастурлардан фойдаланиш;

d) буфернинг тўлиб кетишидани фойдаланадиган ҳужумлардан муҳофаза қилиш.

Тегишли назоратга оид рўйхатни тайёрлаб қўйиш, хатти-ҳаракатларни ҳужжатлаштириш ва натижаларни ишончли сақлаш керак. Текширувнинг ўрнатилган воситаларига қуйидагилар мисол бўлиши мумкин:

a) транзакциялар янгиланганидан сўнг маълумотлар файлларини тўловлар баланси билан мувофиқлаштириш учун сеансли ёки пакетли ишлов беришнинг бошқариш воситалари;

b) кирувчи қолдиқларни олдинги ёпиқ қолдиқлар билан текшириш мақсадида уларни назорат қилиш воситалари, айнан:

1) «бажаришдан-бажаришга» назорат воситалари;

2) файлдаги ўзгартирилган маълумотларнинг умумий суммаси;

3) «дастурдан-дастурга» назорат воситалари;

c) тизим томонидан генерацияланган маълумотларнинг тўғрилигини тасдиқлаш (12.2.1);

d) марказий (асосий) ва узоқлаштирилган компьютерлар ўртасидаги олинган ёки узатилган маълумотларнинг, шунингдек, дастурий таъминотнинг бутлиги, ҳақиқийлигини ёки хавфсизлигининг ҳар қандай бошқа тавсифини текшириш;

e) ёзувлар ва файлларнинг назорат суммалари;

f) амалий дастурлар белгиланган вақтда бажарилаётганлигига ишонч ҳосил қилиш учун текширувлар;

g) дастурлар тўғри кетма-кетликда бажарилаётганлиги ва тўхтаб қолган ҳолда уларнинг бажарилишини тўхтатиш, шунингдек, муаммо ҳал бўлмагунича маълумотларга кейинги ишлов бериш тўхтатилишига кафолат берувчи текширувлар;

h) маълумотларни киритиш жараёнида бажариладиган амалларни рўйхатга олиш журналини юритиш (10.10.1).

Бошқалар

Тўғри киритилган маълумотлар аппарат воситаларининг хатолари, ишлов бериш хатолари ёки атайлаб қилинган хатти-ҳаракатлар натижасида бузилиши мумкин. Тўғриликни текширишни талаб қиладиган текширувлар илованинг турига ва маълумотлар шикастланишининг бизнесга таъсирига боғлиқ.

12.2.3 Хабарларнинг бутлиги

Бошқариш воситаси

Иловаларда хабарларнинг ҳақиқийлигини таъминлаш ва бутлигини муҳофаза қилиш бўйича иловаларга қўйилган талаблар белгиланган бўлиши, шунингдек, тегишли бошқариш воситалари аниқланиши ва жорий этилиши керак.

Жорий этиш бўйича қўлланма

Хабарларни аутентификация қилиш кераклигини аниқлаш учун хавфсизлик хавфларини баҳолаш ва уни амалга оширишнинг энг қулай методини танлаш зарур.

Криптографик методлардан хабарларни аутентификация қилишни амалга оширишнинг лозим бўлган воситаси сифатида фойдаланиш мумкин (12.3).

12.2.4 Чиқувчи маълумотларни текшириш

Бошқариш воситаси

Ахборотга ишлов бериш тўғри бажарилганлигига ишонч ҳосил қилиш учун иловалардан чиқариладиган маълумотларнинг тўғрилигини текшириш зарур.

Жорий этиш бўйича қўлланма

Чиқариладиган маълумотлар тўғрилигининг тасдиғи қуйидагиларни ўз ичига олиши керак:

a) чиқариладиган маълумотларни қабул қилиш мумкинлигини аниқлаш мақсадида тўғрилигини текшириш;

b) барча маълумотларга ишлов берилганлигига амин бўлиш учун назорат ҳисоблагичларини текшириш;

c) чиқариш натижаларини олувчи ёки ишлов беришнинг кейинги тизими ахборотнинг тўғрилигини ва таснифини аниқлаши мумкин бўлиши учун уларни етарли ахборот билан таъминлаш;

d) чиқувчи маълумотларнинг ишончлилиги ва тўғрилигини тестдан ўтказиш натижаларига муносабат билдириш процедуралари;

e) маълумотларни чиқариш жараёнига жалб қилинган барча ходимлар мажбуриятларини белгилаш;

f) маълумотлар чиқарилишининг тўғрилигини текшириш жараёнида бажариладиган амалларни рўйхатга олиш журналини яратиш.

Бошқалар

Одатда, тизимлар текширувлар ва тестдан ўтказишлар тўғрилигининг тегишли тасдиқлари мавжудлигида чиқариладиган маълумотлар доим тўғри бўлади, деган фикрга асосланиб тузилади. Бироқ, ушбу таҳмин ҳар доим ҳам тўғри эмас; яъни баъзи бир ҳолатларда текширилган тизимлар ҳам нотўғри натижа бериши мумкин.

12.3 Муҳофаза қилишнинг криптографик воситалари

Мақсад: ахборотнинг конфиденциаллиги, асл нусхасига мувофиқлиги ва бутлигини криптографик воситалар билан муҳофаза қилиш.

Бошқаришнинг криптографик воситаларидан фойдаланиш сиёсатини ишлаб чиқиш керак. Криптогрфик методларни сақлаш ва улардан фойдаланиш учун калитларни бошқариш принципларини жорий қилиш керак.

12.3.1 Муҳофаза қилишнинг криптографик воситаларидан фойдаланиш сиёсати

Бошқариш воситаси

Ахборотни муҳофаза қилишнинг криптографик воситаларидан фойдаланиш сиёсатини ишлаб чиқиш ва жорий қилиш керак.

Жорий этиш бўйича қўлланма

Криптографик воситалардан фойдаланиш сиёсатини ишлаб чиқишда қуйидагиларни аниқлаш керак:

a) ташкилотда криптографик воситалардан фойдаланиш методикаси, шу жумладан бизнес-ахборот муҳофаза қилиниши керак бўлган умумий принциплар (5.1.1);

b) шифрлашнинг талаб қилинган алгоритмининг тури, бар-қарорлиги ва сифатини эътиборга олган ҳолда хавфларни аниқлашга асосланган муҳофазанинг талаб қилинган даражаси;

c) мобил ёки алмашинувчи ташувчиларда, қурилмаларда олиб юриладиган ёхуд телекоммуникация линиялари бўйича узатиладиган конфиденциал ахборотни муҳофаза қилиш учун шифрлашдан фойдаланиш;

d) калитларни бошқариш принциплари, шу жумладан калитлар йўқотилган, компрометация қилинган ёки шикастланган ҳолда шифрланган ахборотни тиклаш методлари;

e) қуйидагилар учун жавобгар мансабдор шахсларнинг вазифалари ва мажбуриятларини тақсимлаш:

1) сиёсатни амалга ошириш;

2) калитларни бошқариш, жумладан калитларни яратиш (12.3.2);

f) ташкилотда криптомуҳофаза методларини самарали жорий қилишни таъминлаш учун қабул қилиниши керак бўлган стандартлар (қандай ечимлардан фойдаланилади, қандай бизнес-жараёнлар учун);

g) шифрланган ахборотдан фойдаланишнинг таркибни таҳлил қилишга асосланган бошқариш воситаларига таъсири (масалан, вирусларни аниқлаш).

Криптографик воситалардан фойдаланиш сиёсатини ишлаб чиқишда қонун ҳужжатлари талабларини ва турли мамлакатларда криптографик методлардан фойдаланиш борасида қўлланиши мумкин

бўлган чеклашларни, шунингдек, давлатлар чегараси орқали узатиладиган шифрланган ахборот оқимининг ҳажмига тегишли масалаларни ҳисобга олиш зарур (15.1.6).

Бошқаришнинг криптографик воситаларидан хавфсизликнинг турли мақсадларига эришиш учун фойдаланиш мумкин, масалан:

a) конфиденциалликка: сақланадиган ва узатиладиган конфиденциал ва сезгир ахборотни муҳофаза қилиш учун ахборотни шифрлашдан фойдаланиш;

b) бутлик/ҳақиқийликка: сақланадиган ёки узатиладиган конфиденциал ёки сезгир ахборотнинг бутлигини/ҳақиқийлигини муҳофаза қилиш учун электрон рақамли имзолардан ёки хабарни аутентификация қилиш кодларидан фойдаланиш;

c) аппеляция қилинишига: ҳодиса ёки хатти-ҳаракатнинг пайдо бўлиши ёки йўқлигининг исботларини олиш учун криптографик методлардан фойдаланиш.

Бошқалар

Криптографик муҳофазани қўллашга тегишли қарорларга хавф-ларни баҳолаш ва ахборот хавфсизлигини таъминлаш бўйича тадбирларни танлаш умумий жараёнининг таркибий қисми каби қараш керак.

Ушбу баҳодан криптографик воситалар, уларнинг турларини қўллаш мақсадга мувофиқлигини, шунингдек, уларни қандай мақсадда ва қандай бизнес-жараёнлар учун қўллаш кераклигини аниқлаш учун фойдаланилади.

Бошқаришнинг криптографик воситаларидан фойдаланиш сиёсати криптографик методлардан максимал фойда олиш ва фойдаланиш хавфларини минимумга келтириш учун, шунингдек, рухсатсиз ёки ноқонуний фойдаланишга йўл қўймаслик учун зарур. Электрон рақамли имзолардан фойдаланишда тегишли қонун ҳужжатларини, хусусан электрон рақамли имзо юридик мажбурятларни юклайдиган шартларни таърифловчи қонун ҳужжатларини кўриб чиқиш керак (15.1).

Муҳофаза қилишнинг талаб қилинган даражасини ва калитларни бошқариш хавфсиз усулларининг муҳофаза қилинишини таъминловчи ва амалга оширилишини қўллаб-қувватловчи мақбул спецификацияларини таъминлаш учун мутахассисларнинг тавсияларидан фойдаланиш керак (12.3.2).

JTCI SC27 ISO/IEC қўмитаси криптографик бошқарув билан боғлиқ бир неча стандартларни ишлаб чиқди. Бундан кейинги ахборот IEEE P1363 да ва OECD криптографияси бўйича қўлланмада мавжуд.

12.3.2 Калитларни бошқариш

Бошқариш воситаси

Ташкилотда криптографик методлардан фойдаланишни таъминлаш учун калитларни бошқаришни жорий этиш керак.

Жорий этиш бўйича қўлланма

Барча криптографик калитлар ўзгартириш, йўқотиш ва бузилишлардан муҳофазаланган бўлиши керак. Бундан ташқари, махфий ва шахсий калитлар рухсатсиз очишдан муҳофаза қилиниши зарур. Калитларни тайёрлаш, сақлаш ва архивлаштириш учун ишлатиладиган ускуналарни жисмоний муҳофаза қилиш керак.

Криптографик калитларни бошқариш тизими келишилган стандартлар, процедуралар ва қуйидаги хавфсиз методларга асосланган бўлиши керак:

a) турли криптографик тизимлар ва турли иловалардан фойдаланишда калитларни генерациялаш;

b) генерациялаш ва очиқ калитлар сертификатларини олиш;

c) калитларни, жумладан уларни олишда активация қилиш бўйича йўриқномани мўлжалланган фойдаланувчиларга тарқатиш;

d) калитларни сақлаш, жумладан авторизация қилинган фойдаланувчиларнинг калитлардан фойдаланиш ҳуқуқини олиш усули;

e) калитларни алмаштириш ёки янгилаш, жумладан калитларни алмаштириш тартиб қоидалари ва муддатлари;

f) компрометация қилинган калитларга нисбатан хатти-ҳаракатлар тартиби;

g) агар калитлар компрометация қилинган ва фойдаланувчи ташкилотдан бўшаб кетган бўлса (бу ҳолда калитларни архивлаштириш керак), калитларни бекор қилиш, жумладан калитларни бекор қилиш ва дезактивация қилиш усуллари;

h) шифрланган ахборотнинг сирини ошкор қилиш учун йўқотилган ёки бузилган калитларни тиклаш;

i) калитларни архивлаштириш, масалан, архивлаштирилган ёки резервланган ахборот учун;

j) калитларни йўқ қилиш;

k) рўйхатга олиш ва калитларни бошқариш билан боғлиқ хатти-ҳаракатлар аудити.

Калитларни компрометация қилиш эҳтимолини камайтириш учун улардан криптографик воситалардан фойдаланиш ҳолатлари ва ахборотни ошкор қилиш хавфининг даражасига боғлиқ бўлган чекланган вақт оралиғи давомида фойдаланиш мумкин бўлиши учун уларни активизация ва дезактивизация қилиш санаси белгиланган бўлиши зарур.

Махфий ва шахсий калитларни хавфсиз бошқаришга қўшимча равишда очиқ калитларнинг ҳақиқийлигини муҳофаза қилишни кўриб чиқиш зарур. Ушбу ҳақиқийликни текшириш жараёнини, одатда, ишончнинг талаб қилинган даражасини таъминлайдиган тегишли қоидалар ва процедураларга амал қиладиган, расман тан олинган ташкилот бўлиши керак бўлган сертификатлаштириш маркази томонидан бериладиган очиқ калитлар сертификати ёрдамида бажариш мумкин.

Криптографик хизматларнинг ташқи етказиб берувчилари билан, масалан, сертификатлаштириш органи билан тузилган контрактларда

хизматларнинг жавобгарлиги, хизматлар ишончлилиги ва уларнинг тақдим этилиши бўйича сўровларга муносабат билдириш вақти бўйича талаблар киритилган бўлиши зарур (6.2.3).

Бошқалар

Криптографик калитларни бошқариш криптографик методлардан самарали фойдаланиш учун муҳим. ISO/IEC 11770 стандарти калитларни бошқариш бўйича кейинги ахборотни тақдим этади. Криптографик методларнинг иккита тури мавжуд:

а) икки ва ундан ортиқ томон биргаликда битта калитдан фойдаланадиган ва ушбу калит ахборотни шифрлаш каби, дешифровкалаш учун ҳам қўлланадиган жойларда махфий калитларга тегишли методлар. Бу калит сир сақланиши керак, чунки ушбу калитдан фойдалана оладиган ҳар қандай фойдаланувчи калит ёрдамида шифрланган барча ахборотни дешифровкалаши ёки рухсат берилмаган ахборотни киритиши мумкин;

b) ҳар бир фойдаланувчи бир жуфт калитга, очиқ калитга (исталган одам фойдаланиши мумкин бўлган) ва шахсий калитга (сир сақланиши керак бўлган) эга бўлган жойда очиқ калитларга тегишли методлар; очиқ калит билан шифрлаш методлари шифрлаш каби, рақамли имзоларни генерациялаш учун ҳам ишлатилиши мумкин (шунингдек, ISO/IEC 9796 ва ISO/IEC 14888 стандартлари қаралсин).

Электрон рақамли имзоларни соҳталаштириш ва фойдаланувчиларнинг очиқ калитини алмаштириб қўйиш хавфи мавжуд. Ушбу муаммо очиқ калитлар сертификатлари ёрдамида ҳал этилади.

Криптографик методлардан, шунингдек, криптографик калитларни муҳофаза қилиш учун ҳам фойдаланиш мумкин. Криптографик калитлардан юридик асосланган фойдаланишни тақдим этиш имкониятларини кўзда тутиш зарур, масалан, судда исбот сифатида фойдаланиладиган ахборотни расшифровка қилиш учун.

12.4 Тизим файлларининг хавфсизлиги

Мақсад: тизим файлларининг хавфсизлигини таъминлаш.

Тизим файллари ва дастурларнинг бошланғич кодларидан фойдаланишни бошқариш керак, ахборот тизимларини лойиҳалаштириш ва уларни техник кузатишни хавфсиз усулда бажариш керак. Тестдан ўтказишда берк маълумотларнинг ошкор этилишига йўл қўймаслик учун эҳтиёткорликка риоя қилиш керак.

12.4.1 Эксплуатация қилинадиган дастурий таъминотни бошқариш

Бошқариш воситаси

Саноатга оид эксплуатацияга дастурий таъминотни жорий этиш жараёнини бошқариш тартибини жорий этиш керак.

Жорий этиш бўйича қўлланма

Саноатга оид эксплуатациядаги мавжуд тизимларнинг шикастланишини минимумга келтириш учун қуйидаги тавсияларни кўриб чиқиш мақсадга мувофиқ бўлади:

a) дастурларнинг ишчи кутубхоналарини янгилашни фақат тайинланган мутахассис - мажбуриятлари раҳбарият томонидан тегишли равишда авторизация қилинган кутубхоначи бажариши керак (12.4.3);

b) саноатда эксплуатация қилинадиган тизимлар фақат бажарилиши мумкин бўлган дастурий кодларга эга бўлиши керак ва ишлаб чиқиш кодига ёки компиляторларга эга бўлмаслиги керак;

c) иловалар ва операцион тизимларнинг дастурий таъминотларини фақат ҳар томонлама муваффақиятли синовлардан сўнг саноатга оид эксплуатацияга жорий этиш керак; ушбу синовларга амалийлиги, хавф-сизлиги, бошқа тизимларга таъсири ва эксплуатация қилиниши осонлигини текшириш учун тестларни киритиш керак, уларни алоҳида тизимларда (10.1.4) бажариш керак; дастурлар кутубхоналарининг барча тегишли бошланғич матнларини янгилаш керак;

d) барча жорий этилган дастурий таъминотларни, шунингдек, тизим ҳужжатларини бошқаришни таъминлаш учун конфигурацияларни бошқариш тизимидан фойдаланиш керак;

e) ўзгаришларни жорий этишдан олдин бошланғич ҳолатга қайтиш стратегиясининг мавжудлиги таъминланиши керак;

f) саноатга оид эксплуатацияда бўлган дастурлар кутубхоналарининг барча янгиланишлари аудит журналида рўйхатга олиниши зарур;

g) кутилмаган вазиятлар юзага келган ҳолларда тизимни тиклаш учун дастурий таъминотнинг олдинги версиялари сақланиши зарур;

h) дастурий таъминотнинг эски версияларини архивлаштириш ва барча талаб қилинган ахборот ва параметрлар, процедуралар, конфигурациянинг тафсилотлари ва ёрдамчи дастурий таъминот билан бирга сақлаш керак.

Саноатга оид эксплуатацияда ишлатиладиган дастурий таъминот ишлаб чиқувчи томонидан белгиланган даражада сақлаб турилиши зарур. Маълум бир вақт ўтганидан сўнг, дастурий таъминотни ишлаб чиқувчилар дастурий таъминотнинг эски версияларини сақламай қўядилар. Ташкилот қўллаб-қувватланмайдиган дастурий таъминотга боғлиқ хавфларни кўриб чиқиши керак.

Кейинги версияга ўтишда унинг хавфсизлигини эътиборга олиш керак: хавфсизликнинг янги функцияларини қўшиш ёки ушбу версияда хавфсизликни таъминлшга тегишли муаммоларнинг мавжудлиги. Агар дастурий ямоқлар хавфсизлик таҳдидларини йўқотиш ёки камайтириши мумкин бўлса, улардан фойдаланиш мақсадга мувофиқ бўлади (12.6.1).

Жисмоний ёки мантиқий фойдаланиш етказиб берувчилар (ишлаб чиқувчилар)га, заруратга кўра, раҳбарларнинг рухсати бўлгандагина, фақат

дастурий таъминотни сақлаб туриш учун тақдим этилади. Бунда етказиб берувчи (ишлаб чиқувчи)нинг хатти-ҳаракатлари назорат қилиниши керак.

Ташкилот дастурий таъминотининг хавфсизлиги ташкилот хавфсизлигидаги заифликларни активлаштиришга қодир рухсатсиз ўзгаришларнинг мустасно қилиш учун кузатиб борилиши ва бошқарилиши керак бўлган, ташқаридан етказиб бериладиган дастурий таъминотга ва модулларга боғлиқ бўлиши мумкин.

Бошқалар

Операцион тизимлар фақат талабга кўра модернизация қилиниши керак, масалан, агар операцион тизимнинг кундалик версияси бизнес талабларига бошқа жавоб бермаса. Модернизация қилиш фақатгина операцион тизимнинг янги версиясидан фойдаланиш мумкин бўлганлиги учун жоиз бўлмаслиги керак. Операцион тизимларнинг янги версиялари амалдаги тизимларга қараганда камроқ хавфсизроқ, камроқ барқарорроқ ва камроқ тушунарлироқ бўлиши мумкин.

12.4.2 Тизим тест маълумотларини муҳофаза қилиш

Бошқариш воситаси

Тест маълумотларини синчиклаб танлаш ва муҳофаза қилиш, шунингдек, уларни бошқариш керак.

Жорий этиш бўйича қўлланма

Саноатда ишлатиладиган ва шахсий маълумотларга эга бўлган маълумотлар базасидан фойдаланишдан қочиш керак. Агар шахсий ёки бошқа конфиденциал ахборотдан тестдан ўтказиш мақсадлари учун фойдаланилса, талаб этилса, барча конфиденциал элементлар ва унинг ичидагилар фойдаланишдан олдин йўқ қилиниши ёки билиб бўлмайдиган даражада ўзгартирилиши керак. Тестдан ўтказишда операцион тизим маълумотларини муҳофаза қилиш учун қуйидаги тавсияларни бажариш керак:

a) ишчи амалий тизимларда қўлланадиган фойдаланишни бошқариш процедураларини тестдан ўтказиладиган амалий тизимлар учун ҳам қўллаш керак;

b) ишчи ахборотдан тестдан ўтказадиган амалий тизимга ҳар гал нусха кўчирилганда ушбу амалларни авторизация қилиш назарда тутилиши керак;

c) тестдан ўтказиш тугатилганидан сўнг, ишчи ахборотни тестдан ўтказадиган амалий тизимдан дарҳол йўқ қилиш керак;

d) ишчи ахборотдан нусха кўчириш ва ундан фойдаланишни аудит журналида рўйхатга олиш керак.

Бошқалар

Тизимни тестдан ўтказиш ва қабул қилиш синовлари, одатда, эксплуатацион маълумотларга максимал яқинлашган тест маълумотларининг катта ҳажмидан фойдаланишни талаб қилади.

12.4.3 Дастурларнинг дастлабки кодларидан фойдаланишни бошқариш

Бошқариш воситаси

Дастурларнинг дастлабки кодларидан фойдаланиш чекланган бўлиши керак.

Жорий этиш бўйича қўлланма

Рухсатсиз функционал имкониятлар ва атайлаб қилинмаган ўзгаришларни киритишнинг олдини олиш учун дастурларнинг дастлабки кодларидан ва улар билан боғлиқ ҳужжатлардан (лойиҳалар, спецификациялар, текширувлар режалари ва тасдиқлашлар режалари каби) фойдаланишни қатъийлик билан бошқариш керак. Дастурларнинг дастлабки кодлари учун бунга бундай кодларнинг бошқарилувчи марказий тўплагичи ёрдамида эришиш мумкин, кўпинча дастурларнинг дастлабки кодлари кутубхоналарида. Компьютер дастурларининг шикастланиш эҳтимолини камайтириш учун дастурларнинг дастлабки кодлари кутубхоналаридан фойдаланишни бошқариш бўйича тавсияларни (11) кўриб чиқиш керак:

a) дастурларнинг дастлабки кодлари кутубхоналарини иложи борича саноатда экплуатацияда бўлган бизнес-иловалардан алоҳида сақлаш керак;

b) дастурларнинг дастлабки кодлари ва дастлабки кодлар кутубхоналарини белгиланган тартибга мувофиқ бошқариш керак;

c) хизмат кўрсатувчи ходимлар дастурларнинг дастлабки кодлари кутубхоналаридан чекланмаган фойдаланишга эга бўлмасликлари керак;

d) дастурлар дастлабки кодларининг кутубхоналарини ва ассоциацияланган элементларни янгилаш, шунингдек, дастурчиларга дастурларнинг дастлабки кодларини бериш фақат тегишли рухсат олинганидан сўнг амалга оширилиши керак;

e) дастур листингларини хавфсиз жойда сақлаш керак (10.7.4);

f) дастурларнинг дастлабки матнлари кутубхоналаридан барча фойдаланишлар учун аудит журналини юритиш керак;

g) рухсатсиз ўзгартириш киритишнинг олдини олиш мақсадида дастурлар дастлабки матнлари кутубхоналарини сақлаш ва улардан нусха кўчиришни қатъий назорат остида ўтказиш керак (12.5.1).

Бошқалар

Дастурларнинг дастлабки кодлари - бу ижро этиладиган кодларни яратиш учун компиляция қилинадиган (ва компановка қилинадиган) дастурчилар томонидан ёзилган кодлар. Бази бир дастурлаш тиллари дастлабки ва ижро этиладиган кодларни расман ажрата олмайдилар, чунки ижро этиладиган кодлар улар чақирилган пайтда яратилади.

ISO 10007 ва ISO/IEC 12207 стандартлари конфигурацияларни бошқариш ва дастурий таъминотнинг ҳаётий цикли жараёнлари тўғрисидаги ахборотни тақдим этади.

12.5 Ишлаб чиқиш ва таъминлаш жараёнларининг хавфсизлиги

Мақсад: дастурий таъминот ва амалий тизимлар маълумотлари хавфсизлигини таъминлаш. Лойиҳалаштириш ва техник таъминлаш муҳитини қатъий бошқариш керак.

Амалий тизимлар учун жавобгар менежерлар, лойиҳалаштириш ёки техник таъминлаш муҳитининг хавфсизлиги учун ҳам жавобгар бўлишлари керак. Улар тизимнинг барча таклиф қилинган ўзгаришларини таҳлил қилишлари ва тизимнинг ҳамда саноатга оид эксплуатация муҳитининг хавфсизлигини компрометация қилиш имкониятини истисно қилишлари керак.

12.5.1 Ўзгаришларни бошқариш тартиби

Бошқариш воситаси

Ўзгаришларни жорий этишни ўзгаришларни бошқаришнинг расмий жараёни ёрдамида бошқариш керак.

Жорий этиш бўйича қўлланма

Ахборот тизимларининг шикастланишларини минимумга келтириш учун ўзгаришларни бошқаришнинг расмий процедураларини белгилаш, ҳужжатлаштириш ва жорий этиш керак. Мавжуд тизимларга янги тизимларни ва аҳамиятга эга бўлган ўзгаришларни киритиш ҳужжатлаштириш, спецификация қилиш, тестдан ўтказиш, сифатини текшириш ва бошқариладиган жорий этишнинг расмий жараёнига мос келиши керак.

Ушбу жараён хавфларни аниқлашни, ўзгаришлар таъсирининг таҳлилини ва хавфсизликни бошқариш зарур воситаларининг батафсил таърифини ўз ичига олиши керак. Шунингдек, ушбу жараён хавфсизлик ва бошқариш процедуралари компрометация қилинмаганлигини, дастурчилар тизимнинг фақат ўзларининг ишлари учун зарур бўлган қисмларидан фойдаланиш ҳуқуқларига эга эканликларини ва ҳар бир ўзгариш расман келишилган ва маъқулланганлигини кафолатлаши керак.

Мумкин бўлган ҳамма жойда амалий процедуралар ва амалий ҳамда ишга оид тизимларнинг ўзгаришларини бошқариш процедуралари интеграцияланган бўлиши керак (10.1.2). Ўзгаришлар процедуралари қуйидагиларни ўз ичига олиши керак:

a) авторизация қилиш келишилган даражаларининг баённомасини ёзиш;

b) ўзгаришлар фақат тегишли равишда авторизация қилинган фойдаланувчилар томонидан киритилишини таъминлаш;

c) фойдаланиладиган тизимларнинг бутлигини таъминловчи бошқариш механизмлари ва процедураларини таҳлил қилиш;

d) барча дастурий таъминотни, ахборотларни, маълумотлар базаси ва ўзгартириш талаб қилинадиган аппарат воситаларини идентификация қилиш;

e) иш бошлашдан аввал ўзгаришлар учун батафсил таклифларнинг расман маъқулланишига эришиш;

f) авторизация қилинган фойдаланувчилар томонидан таклиф қилинаётган ўзгаришларни улар бевосита амалга оширилгунча қабул қилинишини таъминлаш;

g) ҳар бир ўзгариш тугаганидан сўнг тизим ҳужжатлари комплектини янгилаш ва эски ҳужжатларни архивлаштириш ёки утилизация қилиш;

h) дастурий таъминотнинг барча янгиланишлари учун версияларни назорат қилишни таъминлаш;

i) ўзгаришлар учун барча талабларни аудит журналида рўйхатга олиш;

j) эксплуатацион ҳужжатлар (10.1.1) ва фойдаланиладиган процедураларни киритилган ўзгаришларга мувофиқ коррекция қилиш;

k) ўзгаришларни келишилган вақтда жорий қилиш жараёнини даҳлдор бизнес-жараёнларни бузмасдан амалга ошириш.

Бошқалар

Дастурий таъминотнинг ўзгариши эксплуатацион муҳитга таъсир этиши мумкин.

Яхши амалиёт саноат муҳитидан ва ишлаб чиқариш муҳитидан ажратилган янги дастурий таъминотни тестдан ўтказишни кўзда тутади (10.1.4). Ушбу амалиёт бошқариш воситасини янги дастурий таъминот билан таъминлайди ва тестдан ўтказиш учун фойдаланиладиган эксплуатацион ахборотни қўшимча муҳофаза қилинишини таъминлайди. Ушбу тестдан ўтказиш ямоқлар, сервис пакетларини ва бошқа янгиланишларни ўз ичига олиши керак. Сезгир тизимларда автоматик янгиланишларни қўллаш керак эмас, чунки баъзи янгиланишлар сезгир иловаларни ишдан чиқариши мумкин (12.6).

12.5.2 Операцион тизим ўзгаришларидан сўнг иловаларни техник таҳлил қилиш

Бошқариш воситаси

Операцион тизимга ўзгартиришлар киртилганда, уларнинг ишлаши ва ташкилот хавфсизлигига ҳеч қандай ноҳуш таъсир кўрсатилмаслигига ишонч ҳосил қилиш мақсадида иловаларни таҳлил қилиш ва тестдан ўтказиш зарур.

Жорий этиш бўйича қўлланма

Ушбу жараён қуйидагиларни ҳисобга олиши зарур:

a) бизнес-иловаларни ва бутлик процедураларини бошқариш воситалари операцион тизим ўзгаришлари томонидан компрометация қилинмаганлигига ишонч ҳосил қилиш учун уларни таҳлил қилиш;

b) ҳар йилги таъминлаш режаси ва бюджетда операцион тизим ўзгаришларида амалга оширилиши зарур бўлган тизимларни таҳлил қилиш ва тестдан ўтказиш кўзда тутилганлигига ишонч ҳосил қилиш;

c) операцион тизимнинг ўзгаришлари тўғрисидаги хабарлар ўз вақтида келиб тушишини таъминлаш, бу иш бошлангунча тегишли таҳлилни ўтказишга имкон беради;

d) узлуксиз ишни таъминлаш режасида тегишли ўзгаришларнинг ҳужжатлаштиришни назорат қилиш (14).

Заифликларни кузатиб бориш, шунингдек, ямоқларни ва ишлаб чиқувчиларнинг тузатишларини чиқариш учун жавобгарни тайинлаш керак (12.6).

12.5.3 Дастурлар пакетларига ўзгартиришлар киритишни чеклаш

Бошқариш воситаси

Дастурлар пакетларини модификация қилишдан қочиш ва зарур ўзгартиришларни киритиш билан чекланиш керак. Барча ўзгаришларни қатъий бошқариш керак.

Жорий этиш бўйича қўлланма

Амалий нуқтаи назардан бу қанчалик мумкин бўлса ва бунга қанчалик йўл қўйилса, ишлаб чиқувчи томонидан етказиб бериладиган дастурлар пакетларидан ўзгартириш киритмасдан фойдаланиш керак. Дастурлар пакетига ўзгартиришлар киритиш зарур бўлган жойларда қуйидагиларни ҳисобга олиш керак:

a) ичига ўрнатилган бошқарув воситалари ва бутлигини таъминлаш жараёнларини компрометация қилиш хавфи;

b) ишлаб чиқувчиларнинг розилигини олиш зарурлиги;

c) талаб қилинадиган ўзгаришларни ишлаб чиқувчидан дастурнинг стандартга оид янгиланган кўринишида олиш имконияти;

d) агар ташкилот киритилган ўзгаришлар натижасида дастурий таъминотга келгусида хизмат кўрсатиш учун жавобгар бўлса, дастурий таъминотни сақлаб туришнинг қўшимча чораларини ишлаб чиқиш зарурати.

Катта аҳамиятга эга бўлган ўзгаришлар бўлган ҳолларда асл дастурий таъминотни сақлаб қўйиш, ўзгаришларни эса, аниқ идентификация қилинган нусхасига киритиш керак. Барча рухсат этилган дастурий таъминотнинг тасдиқланган ямоқлари ва амалий янгиланишларнинг энг охирги версияларини ўрнатишни таъминлаш учун дастурий таъминот янгиланишларини бошқариш жараёнини жорий этиш керак (12.6). Барча ўзгаришларни шундай тестдан ўтказиш ва ҳужжатлаштириш керакки, зарур бўлганда дастурий таъминотни келгусида янгилаш учун ундан қайта фойдаланиш мумкин бўлсин. Агар талаб қилинса, ўзгаришлар мустақил баҳоловчи орган томонидан текширилиши ва тасдиқланиши керак.

12.5.4 Ахборотнинг тарқалиши

Бошқариш воситаси

Ахборотнинг тарқалиш имконияти пайдо бўлишининг олдини олиш керак.

Жорий этиш бўйича қўлланма

Ахборотнинг тарқалиш хавфини, масалан, яширин каналларни топиш ва улардан фойдаланиш йўли билан чеклаш учун қуйидагиларни кўриб чиқиш зарур:

a) чиқувчи ташувчилар ва коммуникацияларни яширин ахборот мавжудлигини билиш учун сканлаш;

b) тизимлар ва коммуникацияларнинг ишлашидан ҳар қандай мантиқий хулосалар қилиш имконини олдини олиш учун уларни билинтирмасликка уриниш ва модуляция қилиш;

c) бутлиги юқори ҳисобланадиган дастурий таъминот ва тизимлардан фойдаланиш, масалан, баҳолашдан ўтган маҳсулотдан фойдаланиш (O‘z DSt ISO/IEC 15408:2008);

d) ходимлар ва тизимларнинг амалларини мавжуд қонун ҳужжатлари ва нормаларга зид бўлмаган усуллар билан мунтазам кузатиб бориш;

e) компьютер тизимларида активлардан фойдаланишни кузатиб бориш;

Бошқалар

Яширин каналлар - бу ахборот оқимларини узатиш учун мўлжалланмаган, лекин шунга қарамай тизим ёки тармоқда мавжуд бўлиши мумкин бўлган йўллар. Масалан, телекоммуникациялар баённомасида пакетларида бошқарувчи битлардан сигналлар узатишнинг яширин методи сифатида фойдаланиш мумкин. Табиатан барча мумкин бўлган яширин канлларни олдиндан бартараф қилиш қийин, агар умуман мумкин бўлса. Шунга қарамай, бундай каналлардан кўпинча «троя отлари» дастурида фойдаланилади (10.4.1), шунинг учун троя кодидан муҳофаза қилишнинг қабул қилинган чоралари яширин каналлардан фойдаланиш хавфини камайтиради.

Тармоқдан рухсатсиз фойдланишнинг (11.4), шунингдек, ахборот хизматлари ходимларига (15.1.5) рухсатсиз фойдаланишга халақит қиладиган сиёсат ва процедураларнинг олдини олиш яширин каналлардан муҳофаза қилишга ёрдам беради.

12.5.5 Бегона ташкилот томонидан дастурий таъминотни ишлаб чиқиш

Бошқариш воситаси

Ташкилот дастурий таъминотнинг бегона ташкилот томонидан ишлаб чиқилишини назорат қилиши ва кузатиб бориши керак.

Жорий этиш бўйича қўлланма

Дастурий таъминотни ишлаб чиқиш учун бегона ташкилот жалб қилинган ҳолларда, қуйидаги чораларни қўллаш керак:

a) лицензияланган контрактларнинг мавжудлигини ва дастурларга эгалик ҳуқуқлари ва интеллектуал эгалик ҳуқуқларига риоя қилинишини назорат қилиш(15.1.2);

b) бажарилган ишларнинг сифатини ва тўғрилигини сертификатлаштириш;

c) бегона ташкилот ўз мажбуриятларини бажариши мумкин бўлмаган ҳоллар учун дастлабки матнни депозитга қўйишни кўзда тутган контрактни тузиш;

d) бажарилган ишлар сифати ва аниқлигининг аудитини ўтказиш учун фойдаланиш ҳуқуқини таъминлаш;

e) дастурлар сифатига қўйиладиган талабларни шартнома шаклида ҳужжатлаштириш;

f) «Троя отлари»ни аниқлаш учун дастурни ўрнатишдан олдин тестдан ўтказиш.

12.6 Техник заифликларни бошқариш

Мақсад: ҳаммага маълум техник заифликлардан фойдаланиш хавфини камайтириш.

Техник заифликларни бошқариш стратегияси самарали, мунтазам ва доимо қўлланадиган бўлиши керак. Ушбу стратегиянинг самаралилигини тасдиқлаш учун миқдор ўлчовларини бажариш керак. Муаммолар доирасида операцион тизимлар ва ҳар қандай фойдаланиладиган бошқа иловаларни кўриб чиқиш керак.

12.6.1 Техник заифликларни бошқариш

Бошқариш воситаси

Фойдаланиладиган ахборот тизимларининг техник заифликлари тўғрисидаги ахборотни ўз вақтида олиш, ташкилотнинг бундай заифликларга дучорлигини баҳолаш ва улар билан боғлиқ хавфларга нисбатан тегишли чоралар қабул қилиш керак.

Жорий этиш бўйича қўлланма

Активларнинг кундалик тўлиқ рўйхати (7.1) - техник заифликларни самарали бошқаришнинг дастлабки шарти. Техник заифликларни бошқариш учун дастурий таъминотнинг ишлаб чиқувчилари, версиялар номерлари ва ўрнатилганлигининг (масалан, қандай дастурий таъминот ва қандай тизимларда ўрнатилган) кундалик ҳолати тўғрисида, шунингдек, ташкилотда дастурий таъминот учун жавобгар шахс (шахслар) тўғрисида батафсил ахборот зарур.

Потенциал техник заифлик аниқланган ҳолда тегишли чоралар кўрилиши керак. Техник заифликларни самарали бошқаришни ташкил қилиш учун қуйидагилар зарур:

a) техник заифликларни бошқариш билан боғлиқ вазифалар ва мажбуриятларни аниқлаш ва бошқариш, жумладан заифликларни кузатиб бориш, заифликлар хавфларини аниқлаш, тузатишлар киритиш, ушбу

ишларни мувофиқлаштириш бўйича активлар ва зарур мажбуриятларни кузатиб бориш;

b) тегишли техник заифликларни аниқлаш ва улар тўғрисидаги хабардорликни таъминлаш учун дастурий таъминот ва бошқа технологиялар учун фойдаланиладиган ахборот активларини белгилаш (7.1.1); инвентаризация қилиш натижалари бўйича ёхуд бошқа янги ёки фойдали активларни топишда ахборот активларини янгилаш;

c) техник заифлик тўғрисида хабарларга муносабат билдириш жадвалини белгилаш, балки ташкилот учун долзарб бўлган заифликларга;

d) ташкилотнинг потенциал техник заифлиги аниқланиши билан боғлиқ хавфлар ва кўриладиган чораларни белгилаш; ушбу чоралар заиф тизимларга тузатишлар киритишни ва/ёки бошқаришнинг бошқа воситаларини қўллашни ўз ичига олиши мумкин;

e) техник заифликка (12.5.1) ишлов беришнинг талаб қилинган шошилинчлигига боғлиқ ёки ахборот хавфсизлигининг инцидентларига муносабат билдириш процедураларига мувофиқ ўзгаришларни бош-қариш билан боғлиқ бошқариш воситаларини қўллаб амалларни бажариш (13.2);

f) агар ямоқдан фойдаланиш мумкин бўлса, ямоқни ўрнатиш билан боғлиқ хавфларни баҳолаш (заифлик туфайли юзага келадиган хавфларни ямоқни ўрнатиш хавфлари билан таққослаш керак);

g) ямоқларнинг самарадорлигини ва йўл қўйиб бўлмайдиган ножўя таъсирларининг бўлмаслигини таъминлаш учун уларни ўрнатишдан олдин текшириш ва баҳолаш; агар ҳеч қандай ямоқлардан фойдаланиш мумкин бўлмаса, қуйидагилар каби бошқа бошқариш воситаларини кўриб чиқиш керак:

1) сервисларни ёки заифликлар билан боғлиқ имкониятларни узиб қўйиш;

2) фойдаланишни бошқариш воситаларини мослаштириш ёки қўшиш, масалан, тармоқлар чегараларидаги тармоқлараро экранларни (11.4.5);

3) реал ҳужумларни аниқлаш ёки олдини олиш учун мониторингни кучайтириш;

4) заифлик тўғрисида хабардорликни ошириш;

h) аудит журналларини барча қўлланадиган процедуралар учун сақлаш керак;

i) техник заифликларни бошқариш жараёнининг самарадорлилигини ва натижавийлигини таъминлаш учун уни мунтазам кузатиб бориш ва баҳолаш керак;

j) катта хавфга эга бўлган тизимлар биринчи навбатда эътибор қилинишини талаб қиладилар.

Бошқалар

Кўпгина ташкилотлар учун техник заифликларни бошқариш жараёнини тўғри бажариш мушкул, шунинг учун ушбу жараённи мунтазам кузатиб бориш керак. Ташкилот учун потенциал долзарб бўлган техник

заифликларни аниқлаш учун инвентаризация қилишнинг аниқ натижалари жуда муҳим.

Техник заифликларни бошқаришга ўзгаришларни бошқаришнинг вазифаси сифатида қараш мумкин; ўзгаришларни бошқариш жараёнлари ва процедураларидан техник заифликларни бошқариш манфаатида фойдаланиш мумкин (10.1.2, 12.5.1).

Кўпинча ямоқларни имкони борича тезлаштириб чиқариб, ишлаб чиқувчиларнинг ўзлари катта босим остида бўладилар, шунинг учун, ямоқ муаммони лозим даражада ҳал қилмаслиги мумкин ва унинг салбий ножўя таъсирлари бўлиши мумкин. Шунингдек, баъзи ҳолатларда ямоқ қўлланиши биланоқ, ямоқни ўрнатишни бекор қилиш осон бўлмайди.

Агар ямоқларни тестдан етарли даражада ўтказиш мумкин бўлмаса, масалан, сарф-харажатлар ёки активларнинг етишмаслиги туфайли, бошқа фойдаланувчиларнинг тажрибасига асосланган ўзаро боғлиқ хавфларни баҳолаш мақсадида тузатишлар киритишни кечиктирилишини кўриб чиқиш мумкин.

13 Ахборот хавфсизлиги инцидентларини бошқариш

13.1 Ахборот хавфсизлигининг ҳодисалари ва заифликлари тўғрисидаги хабарлар

Мақсад: фойдаланувчилар томонидан ахборот хавфсизлигининг ҳодисаларини ва ахборот тизимларининг заифликларини аниқлаш ўз вақтида тузатувчи хатти-ҳаракатларни қабул қилиш имкониятини кафолатлаши керак.

Ҳодисалар тўғрисида хабар беришнинг расмий тартиби ва бундан кейинги хатти-ҳаракатлар тартиби жорий этилган бўлиши керак. Барча ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчилари ташкилот активларининг хавфсизлигига салбий таъсир кўрсатиши мумкин бўлган ахборот хавфсизлиги инцидентларининг ҳар хил турлари тўғрисида ахборот бериш процедуралари (хавфсизликнинг бузилиши, таҳдид, тизимнинг заифлиги ёки тўхтаб қолиши) тўғрисида хабардор бўлишлари керак. Ушбу шахслар кузатилаётган ёки таҳмин қилинаётган ҳар қандай ҳодисалар тўғрисида алоқадаги маълум шахсга ёки хавфсизлик маъмурига кечиктирмасдан хабар бериши керак.

13.1.1 Ахборот хавфсизлиги ҳодисалари тўғрисида хабарлар

Бошқариш воситаси

Ахборот хавфсизлиги ҳодисалари тўғрисида кечиктирмасдан бошқаришнинг мақбул каналлари бўйича имкони борича раҳбариятга тез, белгиланган тартибга мувофиқ хабар бериш керак.

Жорий этиш бўйича қўлланма

Ахборот хавфсизлиги ҳодисалари тўғрисида хабар олинганидан сўнг амалга оширилиши керак бўлган инцидентларга муносабат билдириш тартиби ва кейинги хатти-ҳаракатлар тартиби билан бирга ахборот хавфсизлиги ҳодисалари тўғрисида хабар беришнинг расмий тартиби тасдиқланиши зарур. Ахборот хавфсизлиги ҳодисалари тўғрисида хабарларни қабул қилиш учун жавобгар, алоқада бўладиган шахсни тайинлаш керак. Ушбу алоқада бўладиган шахс тўғрисида, ундан доим фойдаланиш мумкинлиги ва унинг адекват ва ўз вақтида муносабат билдириш қобилияти тўғрисида бутун ташкилотнинг хабардор бўлишини таъминлаш керак.

Барча ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчилари ахборот хавфсизлигининг ҳар қандай ҳодисалари тўғрисида хабардор қилиш процедураси билан таниш бўлишлари керак. Улар, шунингдек, алоқадор шахсни ва унга ахборот хавфсизлиги ҳодисалари тўғрисида хабар бериш тартибини билишлари керак. Хабар бериш тартиби қуйидагиларни ўз ичига олиши керак:

a) ахборот хавфсизлигининг бузилиш инцидентларига муносабат билдириш натижалари бўйича тескари боғланиш процедуралари;

b) хабар бериш жараёнини таъминлаш ва ахборот хавфсизлиги ҳодисалари аниқланган ҳолда барча зарур хатти-ҳаракатлар тўғрисида фойдаланувчига эслатиш учун ахборот хавфсизлиги ҳодисалари тўғрисида хабар бериш шакллари;

c) ахборот хавфсизлиги ҳодисалари аниқланган ҳолда ўзини тўғри тутиш, яъни:

1) дарҳол барча муҳим тафсилотларни ёзиб олиш (масалан, номувофиқлик ёки бузилиш тури, учраган бузилиш, экрандаги хабарлар, ғалати ишлаш);

2) хавфсизлик тизимидаги таҳмин қилинаётган камчиликларни тузатишга мустақил уринмасдан, улар тўғрисида дарҳол алоқадор шахсга хабар бериш;

d) хавфсизлик талабларини бузадиган ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчиларига нисбатан кўриладиган, ташкилотда белгиланган интизомий жавобгарлик чораларига ҳаволалар.

Катта хавфга эга бўлган муҳитларда «мажбурлаш тўғрисида хабар бериш»[4] кўзда тутилган бўлиши мумкин, унинг ёрдамида мажбурлаш объекти бўлган фойдаланувчи ушбу муаммони кўрсатиб бериши мумкин. Зўрлаш тўғрисидаги хабарларга муносабат билдириш тартиби бундай хабарлардан далолат берадиган катта хавфга эга бўлган вазиятни акс эттириши керак.

Бошқалар

Ахборот хавфсизлиги ҳодисалари ва инцидентларига мисоллар:

[4] Мажбурлаш тўғрисида хабар бериш - ҳаракат «мажбуран» амалга оширлаётганлиги тўғрисидаги яширин кўрсатма методи.

a) ускуна ёки хизмат кўрсатиш воситаларига кўрсатилмаган хизмат;
b) тизимнинг бузилишлари ёки ўта юкланиш;
c) инсон омили билан боғлиқ хатолар;
d) сиёсатлар ёки қўлланмаларга номувофиқлик;
e) жисмоний хавфсизлик чораларининг бузилиши;
f) бошқариб бўлмайдиган тизим ўзгаришлари;
g) дастурий ва аппарат таъминотидаги тўхтаб қолишлар;
h) фойдаланишнинг бузилиши.

Конфиденциалликка тегишли эҳтиёткорликка риоя қилишда инцидентлар тўғрисидаги ахборотдан фойдаланувчиларнинг хабардорлигини ошириш мақсадида фойдаланиш мумкин (8.2.2), чунки аниқ мисолларда инцидентларнинг мумкин бўлган оқибатларини намойиш этишга, уларга муносабат билдиришга, шунингдек, келгусида уларга йўл қўймасликка имкон беради.

Ахборот хавфсизлигининг бузилиши инцидентларига лозим даражада муносабат билдириш имконига эга бўлиш учун, улар аниқланганидан сўнг иложи борича тезроқ гувоҳлик кўрсатмаларини ва далилларини йиғиш керак (13.2.3).

Тизимнинг тўхтаб қолишлари ёки бошқа аномал ишлаши хавф-сизликка ҳужум ёки ҳақиқатда хавфсизликнинг бузилиши тўғрисида далолат беради, шунинг учун доимо улар тўғрисида ахборот хавфсизлиги ҳодисалари сифатида хабар бериш керак.

Ахборот хавфсизлиги ҳодисалари ва ахборот хавфсизлиги инцидентларини бошқариш тўғрисидаги хабарларга тегишли батафсилроқ ахборот ISO/IEC TR 18044 да мавжуд.

13.1.2 Ахборот тизимларининг заифликлари тўғрисидаги хабарлар

Бошқариш воситаси

Ахборот тизимлари ва хизматларидан фойдаланувчи ходим, субпудратчилар ва бегона ташкилотларнинг фойдаланувчиларидан улар тизим ёки сервислар хавфсизлиги соҳасида ҳар қандай сезилган ёки таҳмин қилинаётган заифликларга эътибор беришлари ва улар тўғрисида хабар қилишларини талаб қилиш зарур.

Жорий этиш бўйича қўлланма

Ахборот хавфсизлиги инцидентларининг олдини олиш учун барча ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчилари кечиктирмасдан ушбу муаммолар тўғрисида раҳбарият ёки бевосита провайдерга қарорлар қабул қилиш учун хабар беришлари керак. Хабар бериш механизми иложи борича осон, қулай ва фойдалана оладиган бўлиши керак. Ҳаммани хавфсизлик тизимидаги таҳмин қилинаётган камчиликларни ҳар қандай ҳолатда ҳам зинхор мустақил тўғрилашга уринмасликлари тўғрисида хабардор қилиш керак.

Бошқалар

Ходимлар, субпудратчилар ва бегона ташкилотларнинг фойдаланувчиларига улар заифликлар мавжудлиги тўғрисидаги ўзларининг шубҳаларини исботлашга ҳаракат қилмасликлари кераклигини айтиш керак. Заифликларни синаш тизимдан потенциал ноҳақ фойдаланиш каби изоҳланиши, шунингдек, ахборот тизими ёки сервисларнинг шикастланишига ва текширувни ўтказган шахснинг юридик жавобгарлигига олиб келиши мумкин.

13.2 Ахборот хавфсизлигининг инцидентлари ва унинг такомиллашувини бошқариш

Мақсад: ахборот хавфсизлиги инцидентларини бошқаришга изчил ва самарали ёндашишни таъминлаш.

Ахборот хавфсизлигининг ҳодисалари ва заиф жойларига шошилинч самарали ишлов бериш мажбуриятлари ва тартибини жорий этиш керак. Уларга муносабат билдириш тариқасида ахборот хавфсизлиги инцидентларини узлуксиз такомиллаштириш, кузатиб бориш, баҳолаш ва тўлиқ бошқариш жараёнини қўллаш керак.

Юридик талабларга мувофиқлигини таъминлаш учун, зарурат бўлганда, далилларни йиғиш керак.

13.2.1 Мажбуриятлар ва тартиб

Бошқариш воситаси

Ахборот хавфсизлиги инцидентларига тез, самарали ва ташкилий муносабат билдирилишини таъминлаш учун мажбуриятларни ва бошқариш тартибини тасдиқлаш керак.

Жорий этиш бўйича қўлланма

Ахборот хавфсизлиги инцидентларини аниқлаш учун ахборот тизимларининг ҳодисалари ва заифликлари тўғрисида хабар беришдан ташқари (13.1) тизимлар, хабарлар ва заифликлар мониторингини ўтказиш керак (10.10.2).

Ахборот хавфсизлиги инцидентларини бошқариш тартиби бўйича қуйидаги тавсияларни кўриб чиқиш керак:

а) ахборот хавфсизлиги инцидентларининг ҳар хил турлари билан ишлаш тартибини тасдиқлаш, жумладан:

1) ахборот тизимларининг тўхтаб қолишлари ва хизмат кўрсатмаслик;

2) зарар келтирувчи код (10.4.1);

3) хизмат кўрсатишдан бош тортиш;

4) бизнеснинг тўлиқ бўлмаган ёки ноаниқ маълумотлари туфайли хатолар;

5) конфиденциаллик ва бутликнинг бузилиши;

6) ахборот тизимларидан рухсатсиз фойдаланиш;

b) кутилмаган ҳодисаларга муносабат билдиришнинг оддий режаларига қўшимча равишда (14.1.3), тартиб, шунингдек, қуйидагиларни қамраб олиши керак (13.2.2):

1) инцидент сабабларини таҳлил қилиш ва идентификация қилиш;

2) инцидентнинг тарқалишини чеклаш;

3) агар зарур бўлса, инцидент такрорланишининг олдини олиш бўйича тузатувчи таъсирни режалаштириш ва жорий қилиш;

4) инцидентдан сўнг тиклаш жараёнида қатнашувчи ёки ушбу жараёнга жалб этилган шахслар билан алоқа;

5) хатти-ҳаракатлар тўғрисида тегишли давлат органларига хабар бериш;

c) зарурат бўлганда, қуйидагилар учун баённомалар ва бошқа ўхшаш далилларни йиғиш ва сақлаш (13.2.3):

1) муаммоларнинг ички таҳлили;

2) шартнома шартлари, норматив талабларнинг потенциал бузилиши ёки фуқаролик ёки жиноий терговларда, масалан, компьютерлардан рухсатсиз фойдаланишда ёки маълумотларни муҳофаза қилиш бўйича қонун ҳужжатлари бузилганда судда далил сифатида фойдаланиш;

3) дастурий таъминот ва хизмат кўрсатишнинг ишлаб чиқарувчиларидан компенсацияни ушлаб қолиш;

d) хавфсизлик бузилганидан сўнг тиклаш ва тизимнинг бузилишларини тузатиш бўйича чораларни диққат билан ва расман бошқариш керак; тартиб қуйидагиларни таъминлаши керак:

1) саноатга оид тизимлар ва маълумотлардан фойдаланишга фақат аниқ белгиланган ва вакил қилинган ходимга рухсат бериш (6.2);

2) барча кўрилган оператив чораларни батафсил ҳужжатлаштириш;

3) оператив чоралар ва уларни ташкилий равишда кўриб чиқиш тўғрисида раҳбариятга хабар қилиш;

4) бизнес тизимлари ва бошқариш воситаларининг бутлигини минимал кечиктириш билан тасдиқлаш.

Ахборот хавфсизлиги инцидентларини бошқариш мақсадларини раҳбарият билан келишиш, шунингдек, ахборот хавфсизлиги инцидентларини, инцидентлар билан ишлаш бўйича ташкилот устуворлигини бошқариш учун жавобгар ходимларнинг тушунишини таъминлаш керак.

Бошқалар

Ахборот хавфсизлигининг инцидентлари ташкилот ва давлат ташқарисига чиқиши мумкин. Инцидентларга муносабат билдириш билан боғлиқ барча хатти-ҳаракатларни, агар улар ташқи ташкилотлар билан ушбу инцидентлар тўғрисида ахборот алмашиш масалаларига тегишли бўлганда ҳам, мувофиқлаштириш зарур.

13.2.2 Ахборот хавфсизлиги инцидентларини ўрганиш

Бошқариш воситаси

Инцидентлар ва уларнинг сони, тури, параметрлари, шунингдек, бу билан боғлиқ харажатларга тегишли тўхтаб қолишларнинг мониторингини ўтказиш ва рўйхатга олиш тартибини белгилаш зарур.

Жорий этиш бўйича қўлланма

Такрорланадиган ёки энг муҳим инцидентлар ёки тўхтаб қолишларни идентификация қилиш учун ахборот хавфсизлиги инцидентларини баҳолаш ахборотидан фойдаланиш керак.

Бошқалар

Ушбу ахборот бўлғуси инцидентлардан етказилиши мумкин бўлган зарар ва харажатларнинг такрорланишини ва катталигини минимумга келтириш мақсадида ахборот хавфсизлигини бошқариш бўйича мавжуд ёки жорий этилаётган қўшимча тадбирларни такомиллаштиришда ёрдам бериши мумкин. Бундан ташқари, ушбу ахборотни ахборот хавфсизлиги сиёсатини қайта кўриб чиқишда ҳисобга олиш керак (5.1.2).

13.2.3 Далилларни йиғиш

Бошқариш воситаси

Ахборот хавфсизлигининг инциденти инсон ёки ташкилотга қарши суд терговига (фуқаролик ёки жиноий) олиб келиши мумкин бўлган ҳолда, келтирилган далиллар тегишли ҳуқуқий нормаларда баён этилган далилларни йиғиш талабларига ёки ушбу масала кўриладиган муайян суд талабларига мос келиши зарур.

Жорий этиш бўйича қўлланма

Ташкилотда интизомий чораларни қўллаш мақсадида далилларни йиғиш ва тақдим этишда риоя қилиниши керак бўлган ички қоидаларни ишлаб чиқиш керак.

Умумий ҳолда ушбу қоидалар қуйидагиларни назарда тутади:

a) далилларнинг жоизлиги: улардан ҳақиқатда ҳам судда фойдаланиш мумкинми ёки йўқми;

b) далилларнинг аҳамиятга эгалиги: уларнинг сифати ва тўлиқлиги.

Далилларнинг яроқлилигига эришиш учун ташкилот ахборот тизимларини ҳар қандай нашр қилинган стандартларга ёки мақбул далилларнинг амалиётига мувофиқлигини таъминлаши керак.

Тақдим этилган далилларнинг аҳамиятга эга эканлиги мақбул талабларга мос келиши керак. Далилларнинг аҳамиятга эга эканлигини таъминлаш учун тикланиши керак бўлган далиллар сақланган ва ишлов берилган давр мобайнида далилларнинг тўғри ва кетма-кет муҳофаза қилиниши (яъни жараёнларни бошқариш исботлари) учун бир қатор ишонарли исботлар бошқариш воситасининг сифати ва тўлиқлигини кўрсатиши керак. Умуман бунга қўйидаги тарзда эришилади:

a) қоғоз ҳужжатлар учун: асл нусхаси хавфсиз усулда сақланади. Журналда ҳолат содир бўлган сана ва ҳолатлар кўрсатилиб, ҳужжатдан фойдаланиш ҳуқуқини олган шахслар ва рўйхатга олган шахс қайд

этилади. Ҳар қандай текширув асл нусхалари бузилмаганлигини кафолатлаши керак;

b) компьютер ташувчилардаги ахборот учун: ахборотдан фойдаланиш мумкинлигини кафолатлаш учун ҳар бир алмашиниладиган ташувчининг, шунингдек, қаттиқ дисклар ёки компьютернинг асосий хотирасидаги ахборотнинг нусхалари кўчирилиши керак. Нусха кўчириш жараёнида бажарилган барча амаллар журналини сақлаш зарур, нусха кўчириш жараёнининг ўзини ҳужжатлаштириш керак. Ташувчиларининг битта нусхасини ва журнални хавфсиз усулда сақлаш керак.

Тергов бўйича ҳар қандай ишни далилий материалларнинг нусхасида бажариш керак. Бутун далилий базанинг бутлигини муҳофаза қилиш керак. Далилий материалдан нусха кўчиришни ишонарли ходим назорат қилиши керак; шунингдек, нусха кўчириш жараёни қачон ва қаерда бажарилганлиги, нусхани ким кўчирганлиги ва қандай асбоб ва дастурлардан фойдаланилганлиги тўғрисидаги ахборотни протоколлаштириш керак.

Бошқалар

Биринчи марта содир бўлган инцидент аниқланганда у суд терговига олиб келиши мумкинлиги яққол кўзга ташланмайди, шунинг учун инцидентнинг жиддийлигини тушуниб етишдан олдин зарур далилни йўқ қилиш хавфи мавжуд. Мўлжалланган суд терговларида инцидентни аниқлашнинг энг бошланғич босқичида талаб қилинган исботларга тегишли маслаҳатни олиш мақсадида юрист ёки милицияни жалб қилиш мақсадга мувофиқ.

Далил ташкилот чегарасидан ташқарига ва/ёки идоравий бўйсунувидаги чегаралардан чиқиши мумкин. Бундай ҳолларда шунга амин бўлиш керакки, ташкилот талаб қилинган ахборотни далил сифатида йиғиши мумкин. Далилларни тегишли судда қабул қилиш имкониятини ошириш учун, шунингдек, турли судларнинг талабларини кўриб чиқиш керак.

14 Ташкилот узлуксиз ишининг таъминланишини бошқариш

14.1 Узлуксиз ишни таъминлашни бошқаришда ахборот хавфсизлиги масалалари

Мақсад: ишлаб чиқариш фаолиятида тўхтаб қолишига қарши хатти-ҳаракат ва сезгир бизнес-жараёнларни ахборот тизимининг аҳамиятга эга бўлган бузилишларидан ёки фавқулодда вазиятлар оқибатларидан муҳофаза қилиш, шунингдек, ишни ўз вақтида тикланишини кафолатлаш.

Узлуксиз ишни бошқариш профилактик ва тикловчи тадбирларни бирлаштириш ёрдамида фавқулодда вазиятлар ва хавфсизликнинг бузилиши натижасида юзага келган (масалан, табиий офатларнинг, бахтсиз

ҳодисаларнинг, ускуналарнинг тўхтаб қолиши ва атайлаб қилинган хатти-ҳаракатларнинг натижаси бўлиши мумкин бўлган), салбий оқибатларни мақбул даражагача минимумга келтириш мақсадида амалга оширилиши керак. Ташкилотнинг сезувчан жараёнларини белгилаш ва ахборот хавфсизлигини бошқариш бўйича узлуксиз ишлар талабларини операциялар, ходимлар, материаллар, транспорт ва ускуна каби масалаларга тааллуқли узлуксизликнинг бошқа талаблари билан бирлаштириш керак.

Фавқулодда вазиятлар, хавфсизликнинг бузилиши ва хизмат кўрсатишдан бош тортишлар оқибатларини таҳлил қилиш зарур. Бизнес жараёнлар бузилганда уларни талаб қилинган вақт мобайнида тиклаш мақсадида узлуксиз ишни таъминлаш режаларини ишлаб чиқиш ва жорий этиш зарур. Ахборот хавфсизлиги ташкилотдаги барча бошқариш жараёнларининг таркибий қисми бўлиб қолиши учун бундай режаларни қўллаб-қувватлаш ва амалда қўллаш керак.

Узлуксиз ишни бошқариш идентификация қилиш тадбирларини ва хавфларни камайтиришни, бузувчи инцидентлар оқибатларини чеклашни ва асосий бизнес-операцияларнинг ўз вақтида янгиланишини таъминлашни ўз ичига олиши зарур.

14.1.1 Узлуксиз ишни бошқариш жараёнига ахборот хавфсизлигини киритиш

Бошқариш воситаси

Узлуксиз ишни таъминлаш учун ташкилотнинг узлуксиз иши учун зарур бўлган ахборот хавфсизлиги талабларини бажаришга қаратилган бошқариладиган жараённи ишлаб чиқиш ва бутун ташкилотда сақлаб туриш керак.

Жорий этиш бўйича қўлланма

Ушбу жараён узлуксиз ишни бошқаришнинг асосий элементларини бирлаштириши керак:

a) ташкилот дуч келадиган хавфларни пайдо бўлиш эҳтимоли ва оқибатлари нуқтаи назаридан тушуниш, жумладан критик бизнес-жараёнларнинг устуворлигини идентификация қилиш ва белгилаш (14.1.2);

b) сезгир бизнес-жараёнларда амалда бўлган барча активларни аниқлаш (7.1.1);

c) арзимаган ёки ташкилотнинг ҳаёт фаолиятига потенциал хавф туғдирадиган катта аҳамиятга эга бўлган инцидентлар содир бўлганда бизнес-жараёнлар бузилишининг мумкин бўлган оқибатларини тушуниш, шунингдек, бизнес мақсадларига мувофиқ келадиган ахборотга ишлов бериш воситалари ва усулларини танлаш;

d) узлуксиз ишни таъминлаш жараёнининг бир қисми, шунингдек, операцион хавфларни бошқаришнинг бир қисми бўлиши керак бўлган ахборотга ишлов бериш натижаларини оптимал суғурта қилишни ташкил қилиш;

e) бошқаришнинг қўшимча огоҳлантирувчи ва юмшатувчи бошқариш воситаларининг жорий қилинишини аниқлаш ва кўриб чиқиш;

f) ахборот хавфсизлигининг белгиланган талабларини қондириш учун етарли молиявий, ташкилий, техник активларни ва атроф-муҳит активларини аниқлаш;

g) ходимларнинг хавфсизлигини, ахборотга ишлов бериш воситалари ва ташкилот мулкининг муҳофазасини таъминлаш;

h) келишилган сиёсатга мувофиқ ахборот хавфсизлигининг талабларини таъминлашга қаратилган узлуксиз ишни таъминлаш режаларини ифодалаш ва ҳужжатлаштириш (14.1.3);

i) ахборот технологияларини ривожлантириш режаларини ва мавжуд жараёнларни мунтазам тестдан ўтказиш ва янгилаш (14.1.5);

j) узлуксиз ишни бошқаришни ташкилот жараёни ва структурасига киритишни кафолатлаш; узлуксиз ишни бошқариш жараёни учун жавобгарликни ташкилот ичидаги ваколатли шахсга юклаш керак (6.1.1).

14.1.2 Ишнинг узлуксизлиги ва хавфларни аниқлаш

Бошқариш воситаси

Ахборот хавфсизлиги учун бизнес жараёнларининг узилиши ва оқибатларининг эҳтимоли ҳамда таъсир даражаси билан бир қаторда бизнес жараёнларининг узилишини келтирб чиқаришга қодир ҳодисаларни аниқлаш керак.

Жорий этиш бўйича қўлланма

Ахборот хавфсизлигига тегишли бўлган узлуксиз иш масалаларини ташкилот бизнес жараёнларининг узилишини келтириб чиқаришга қодир ҳодисалар (ёки ҳодисалар кетма-кетлигини), масалан, ускунанинг бузилиши, инсон хатолари, ўғирликлар, ёнғин, табиий офатлар ва террористик актларни идентификация қилишда асослаш керак. Бу шикастланиш ва тикланиш даври масштаби нуқтаи назаридан бундай ҳодисаларнинг бўлиши мумкин бўлган оқибатларини аниқлаш мақсадида хавфларни баҳолаш билан кузатилиши керак.

Хавфларни баҳолашни бевосита бизнес-ресурслар эгалари ва бизнес-жараёнлар қатнашчилари иштирокида амалга ошириш керак. Хавфларни баҳолаш барча бизнес-жараёнларга тааллуқли бўлиши ва фақат ахборотга ишлов бериш воситалари билан чекланиб қолмаслиги керак, ахборот хавфсизлиги учун хос бўлган натижаларни ҳисобга олиш керак. Хавфнинг турли томонларини бирга боғлаш ва ташкилот узлуксиз иши талабларининг тўлиқ тавсифини олиш муҳим. Ушбу баҳо хавфларни аниқлаши, ташкилот учун мақбул мезонлар ва мақсадларга нисбатан устуворликлари, жумладан сезгир активлари, бузилишлар таъсири, электр таъминоти узиб қўйилишининг йўл қўйилган вақти ва тиклаш устуворликлари бўйича ўлчаши ва жойлаштириши керак.

Хавфларни баҳолаш натижаларига боғлиқ ҳолда узлуксиз ишни таъминлашга умумий ёндошувни белгилайдиган режани ишлаб чиқиш

керак. Ишлаб чиқилган режа ташкилот раҳбари томонидан тасдиқланган бўлиши керак.

14.1.3 Ахборот хавфсизлигининг белгиланган талабларини ҳисобга олган ҳолда узлуксиз ишни таъминлаш режаларини ишлаб чиқиш ва жорий этиш

Бошқариш воситаси

Узлуксиз ишни таъминлаш ва бизнес-операцияларни тиклаш режаларини талаб қилинган вақт ичида муҳим сезгир бизнес-жараёнларнинг узилиши ёки тўхтаб қолишидан сўнг ишлаб чиқиш керак.

Жорий этиш бўйича қўлланма

Узлуксиз ишни таъминлаш режаси қуйидаги тадбирларни кўзда тутиши зарур:

a) фавқулодда вазият ҳолатида мансабдор шахсларнинг барча мажбуриятларини ва барча процедураларни аниқлаш ва келишиш;

b) ахборот ва хизматларнинг мақбул йўқотишларини аниқлаш;

c) бизнес-жараёнларни талаб қилинган вақт ичида тиклаш имконини таъминлайдиган авария процедураларини амалга ошириш; алоҳида эътиборни бизнеснинг ташқи омиллар ва мавжуд контрактларга боғлиқлик баҳосига қаратиш керак;

d) бизнес-жараёнларнинг тикланиши ва янгиланиши тугашини кутишда бажариладиган ишга оид процедуралар;

e) келишилган процедуралар ва жараёнларни ҳужжатлаштириш;

f) ходимларни фавқулодда вазият рўй берган пайтида хатти-ҳаракатларга, жумладан инқироз ҳолатида бошқаришга ўргатиш;

g) узлуксиз ишни таъминлаш режаларини тестдан ўтказиш ва янгилаш.

Режалаш жараёнида диққат эътиборни бизнеснинг талаб қилинган мақсадларига, масалан, мижозлар учун мақбул вақт оралиғида муайян сервисларни тиклашга қаратиш керак. Ахборотга ишлов бериш воситалари учун ходимлар, резерв русурлар билан комплектлашни, шунингдек, ушбу воситалар учун ишнинг авария режимига ўтиш бўйича чораларни ҳисобга олган ҳолда, ушбу мақсадларга эришишни енгиллаштирадиган хизматлар ва активларни белгилаш керак. Авария режимига ўтиш бўйича бундай чоралар учинчи шахслар билан ўзаро келишувлар шаклидаги контрактларни ёки абонентлик обунасининг тижорат хизматларини ўз ичига олиши мумкин.

Узлуксиз ишни таъминлаш режаларида ташкилотнинг заифликларини кўрсатиш керак ва шунинг учун ушбу режалар тегишли равишда муҳофаза қилиниши керак бўлган конфиденциал ахборотга эга бўлиши мумкин. Узлуксиз ишни таъминлаш режаларининг нусхаларини асосий объектдаги авариядан ҳар қандай шикастланишининг олдини олиши учун етарли масофада узоқлаштирилган жойда сақлаш керак. Раҳбарият ушбу нусхаларнинг асосий объектдагидек хавфсизлик даражасида муҳофаза қилинишини таъминлаши керак. Шунингдек,

узлуксиз ишни таъминлаш режаларини бажариш учун зарур бўлган бошқа материал ҳам узоқлаштирилган жойда сақланиши керак.

Агар вақтинчалик мақбул жойлардан фойдаланилса, ушбу жойларда жорий этилган хавфсизликни бошқариш воситаларининг даражаси асосий объект даражасига тенг бўлиши керак.

Бошқалар

Шуни айтиб ўтиш керакки, инқирозга қарши бошқариш режалари ва хатти-ҳаракатлари (14.1.3.f) узлуксиз ишни бошқаришдан фарқ қилиши мумкин; яъни мумкин бўлган инқирозга оддий бошқариш процедураларига мувофиқ ишлов берилиши мумкин.

14.1.4 Узлуксиз ишни таъминлаш режаларининг структураси

Бошқариш воситаси

Барча режаларнинг зид эмаслигини таъминлаш ва ахборотга ишлов бериш воситалари ва тизимларига хизмат кўрсатиш ва тестдан ўтказиш учун устуворликларни аниқлаш мақсадида узлуксиз ишни таъминлаш режаларининг ягона структурасини қўллаб-қувватлаш керак.

Жорий этиш бўйича қўлланма

Узлуксиз ишни таъминлашнинг ҳар бир режасида таъминлашга ёндашишни, масалан, ахборотдан ёки ахборот тизимларидан фойдалана олишликни ва хавфсизликни кафолатлашини таърифлаш керак. Узлуксиз ишни таъминлашнинг ҳар бир режаси уни амалга ошириш шартларини, шунингдек, ҳар бир пунктининг бажарилиши учун жавобгар мансабдор шахсларни белгилаши керак. Янги талаблар аниқланганда фавқулодда вазият ҳолатлари учун процедураларга тегишли ўзгартиришлар киритиш керак, масалан, эвакуация қилиш режаларига ёки ишнинг авария режимига ўтиш бўйича ҳар қандай мавжуд режаларга. Узлуксиз иш масалаларига керакли эътиборни таъминлаш учун процедураларни ташкилот ўзгаришларини бошқариш сиёсатига киритиш керак.

Ҳар бир режага муайян раҳбар (ходим) жавоб бериши зарур. Фавқулодда тадбирлар, қўлда ишлов беришнинг авария режимига ўтиш бўйича режалар, ишни янгилаш бўйича режаларни тегишли бизнес ресурсларнинг эгалари ёки даҳлдор жараёнлар қатнашчиларининг жавобгарлик доирасига киритиш керак. Ахборот ва телекоммуникацияга ишлов бериш каби резерв техник воситалардан фойдаланган ҳолда ишнинг авария режимига ўтиш бўйича чоралар учун хизматлар провайдерлари жавобгардир.

Узлуксиз ишни таъминлаш режаларининг структурасида ахборот хавфсизлигининг белгиланган талаблари ҳисобга олиниши ва қуйидагилар кўзда тутилиши зарур:

а) режанинг ҳар бир бандини амалга киритишдан олдин бажарилиши керак бўлган жараён таърифланган (вазиятни қандай баҳолаш керак, кимлар қатнашиши керак ва ҳ.) режаларни амалга ошириш шартлари;

b) бизнес-операцияларни хавфга қўядиган инцидентлардан кейин қўлланиши керак бўлган фавқулодда вазият ҳолатлари учун процедуралар;

c) муҳим бизнес-операциялар ёки хизмат кўрсатиш сервисларини вақтинчалик жойлашиш жойига кўчириш ва бизнес-жараёнларни талаб қилинган вақт оралиғида тиклаш бўйича зарур амалларни таърифлайдиган ишнинг авария режимига ўтиш процедуралари;

d) бизнес-жараёнларнинг тикланиши ва янгиланишини кутишда бажарилиши керак бўлган вақтинчалик ишга оид процедуралар;

e) бизнесни юритишнинг нормал режимига қайтиш учун зарур хатти-ҳаракатларни таърифлайдиган ишни янгилаш процедуралари;

f) тестдан ўтказиш муддатлари ва методларини, шунингдек, режани таъминлаш жараёнининг таърифини белгилайдиган режани таъминлаш графиги;

g) ходимларни ўқитиш бўйича, узлуксиз ишни таъминлаш жараёнларини тушунишига ва ушбу жараёнларнинг доимий самарадорлигини таъминлашга йўналтирилган тадбирлар;

h) режанинг ҳар бир пункти бажарилишига жавобгар мансабдор шахсларнинг мажбуриятлари. Зарур бўлганда мақбул номзодлар кўрсатилган бўлиши керак;

i) сезгир активлар ва фавқулодда процедураларни, авария режимига ўтиш процедураларини ва янгилаш процедураларини бажаришга қодир активлар.

14.1.5 Узлуксиз ишни таъминлаш бўйича режаларни тестдан ўтказиш, техник хизмат кўрастиш ва қайта кўриб чиқиш

Бошқариш воситаси

Узлуксиз ишни таъминлаш режаларининг актуаллиги ва самаралилигини таъминлаш учун уларни мунтазам текшириб ва янгилаб туриш керак.

Жорий этиш бўйича қўлланма

Узлуксиз ишни таъминлаш режаларини текширишда тиклаш командасининг барча аъзолари ва шунга алоқадор бўлган бошқа ходимлар бизнеснинг узлуксизлиги ва ахборот хавфсизлиги учун ўзларининг мажбуриятлари ва жавобгарликлари тўғрисида хабардорликлари, шунингдек, режани амалга киритишда ўзларининг вазифаларини билишларига амин бўлиш керак.

Узлуксиз ишни таъминлаш режаси(лари)ни текшириш графиги режанинг ҳар бир банди қачон ва қандай текширилиши кераклигини белгилаб бериши керак. Режа(лар)нинг айрим бандларини текшириш даврийлиги турлича бўлиши мумкин.

Ҳақиқий ҳаётда режа(лар)нинг ишлашини таъминлашнинг турли методларидан фойдаланиш керак. Бунда қуйидаги методлардан фойдаланиш мумкин:

a) турли сценарийларни тестдан ўтказиш («ишлашини имитация қилиш») (мумкин бўлган фавқулодда вазиятларнинг турли мисолларида бизнесни тиклаш бўйича чораларни муҳокама қилиш);

b) моделни тайёрлаш (айниқса инцидент ва инқироз ҳолатидаги бошқаришга ўтишдан сўнг ходимларни ўз вазифаларини бажаришга ўргатиш учун);

c) техник тиклашни тестдан ўтказиш (ахборот тизимларини самарали тиклашга ишонч ҳосил қилишни таъминлаш);

d) вақтинчалик жойлашиш жойида тиклашни текшириш (бизнес-жараёнлар доимий жойлашиш жойида тиклаш бўйича операциялар билан параллел амалга оширлади);

e) воситалар ва сервислар-етказиб берувчиларни тестдан ўтказиш (бегона ташкилотлар томонидан тақдим этилган сервислар ва дастурий маҳсулотлар контракт мажбуриятларини қониқтиришига ишонч ҳосил қилиш);

f) «энг охирги репетициялар» (ташкилот, ходимлар, ускуна, воситалар ва жараёнлар фавқулодда вазиятларнинг уддасидан чиқишини тестдан ўтказиш);

Тестдан ўтказиш методлари исталган ташкилот томонидан фойдаланилиши мумкин ва улар узлуксиз ишни таъминлаш бўйича муайян режанинг ўзига хос хусусиятларини акс эттириши зарур. Текширувлар натижаларини рўйхатдан ўтказиш керак ва зарур бўлган жойда режаларни яхшилаш бўйича амалларни қўллаш керак.

Узлуксиз ишни таъминлаш бўйича режалар мунтазам қайта кўриб чиқилиши учун жавобгарларни тайинлаш зарур; узлуксиз ишни таъминлаш бўйича режаларда ҳали акс эттирилмаган бизнес-жараёнлардаги аниқланган ўзгаришлар ушбу режаларни тегишли равишда янгилаш йўли билан ҳисобга олинган бўлиши керак. Ўзгаришларни бошқаришнинг расмий жараёни янгиланган режаларни мунтазам қайта кўриб чиқиш доирасида уларнинг тарқатилиши ва амалга киритилишини таъминлаши керак.

Режаларни янгилашни талаб қилиши мумкин бўлган вазиятларнинг мисоллари янги ускунани сотиб олишни ёки операцион тизимларни янгилашни, шунингдек, қуйидагилар билан боғлиқ ўзгаришларни ўз ичига олади:

- ходимлар;
- манзиллар ёки телефон номерлари;
- бизнес стратегияси;
- коммуникация воситалари ва активларнинг жойлашган жойи;
- қонун ҳужжатлари;
- пудратчилар, етказиб берувчилар ва асосий мижозлар;
- жараёнлар (янгилари ва олиб қўйилганлари);
- хавфлар (операцион ва молиявий).

15 Талабларга мувофиқлик

15.1 Қонун ҳужжатлари талабларига мувофиқлик

Мақсад: жиноий ва фуқаролик ҳуқуқлари нормалари, мажбурий кўрсатмалар ва раҳбарий ҳужжатлар талаблари ёки шартнома мажбуриятларининг, шунингдек, ҳар қандай хавфсизлик талабларининг ҳар қандай бузилишининг олдини олиш.

Ахборот тизимларини лойиҳалаштириш ва уларнинг ишлаши, улардан фойдаланиш ва уларни бошқариш мажбурий кўрсатмалар, раҳбарий ҳужжатлар талабларининг, шунингдек, шартнома мажбуриятларидаги хавфсизлик талабларининг предмети бўлиши мумкин.

Муайян юридик масалаларда тегишли малакага эга бўлган ташкилот юристлари ёки тажриба орттираётган юристлар билан маслаҳатлашиш керак. Шуни назарда тутиш керакки, бир мамлакатда яратилган ва бошқасига узатилган (масалан, мамалакат чегарасидан ташқарига узатиладиган ахборот оқими), ахборотга тегишли қонун талаблари турли мамлакатларда турлича.

15.1.1 Қўлланадиган қонун ҳужжатларини аниқлаш

Бошқариш воситаси

Қонун ҳужжатларининг барча қўлланадиган нормалари, мажбурий кўрсатмалар, раҳбарий ҳужжатлар шартнома мажбуриятларини ҳар бир ахборот тизими ва ташкилот учун аниқ белгилаш ва ҳужжатлаштириш керак.

Жорий этиш бўйича қўлланма

Ахборот хавфсизлигини таъминлаш бўйича муайян тадбирлар ва ушбу талабларни бажариш бўйича мансабдор шахсларнинг шахсий мажбуриятларини тегишли равишда белгилаш ва ҳужжатлаштириш керак.

15.1.2 Интеллектуал мулкка эгалик ҳуқуқлари

Бошқариш воситаси

Муаллифлик ҳуқуқи, лойиҳага эгалик ҳуқуқи, савдо маркалари, шунингдек, лицензион дастурий таъминотдан фойдаланиш каби интеллектуал эгалик ҳуқуқи мавжуд бўлиши мумкин бўлган материалдан фойдаланиш учун қонун ҳужжатларидаги чеклашларга мувофиқликни таъминлайдиган процедураларни жорий қилиш зарур.

Жорий этиш бўйича қўлланма

Интеллектуал мулк эгалиги каби баҳоланиши мумкин бўлган ҳар қандай материални муҳофаза қилиш бўйича қуйидаги тавсияларни кўриб чиқиш керак:

а) дастурий ва ахборот маҳсулотларидан қонуний фойдаланишни белгилайдиган дастурий таъминотнинг муаллифлик ҳуқуқига қўйиладиган талабларга қатъий риоя қилиш;

b) муаллифлик ҳуқуқларига риоя қилинишини таъминлаш учун дастурий таъминотни фақат таниқли ва ҳурматга сазовор ишлаб чиқувчилардан сотиб олиш;

c) дастурий таъминотга муаллифлик ҳуқуқи, сотиб олишларга тегишли қабул қилинган қоидалар масалалари бўйича ходимларнинг хабардорлигини таъминлаш, шунингдек, қоидабузарларга интизомий санкциялар қўлланиши тўғрисида хабардор қилиш;

d) интеллектуал мулкка эгалик ҳуқуқларини муҳофаза қилиш талаблари бўлган активларнинг тегишли рўйхатларини сақлаш ва аниқлаш;

e) лицензиялар, дистрибутив дисклар, қўлланмалар ва ҳоказоларга эгалигини тасдиқлаш ва исботлашни бошқариш;

f) дастурий маҳсулот рухсат этилган фойдаланувчиларининг максимал сонини чеклашга риоя қилинишини назорат қилиш;

g) фақат авторизация қилинган дастурий таъминот ва лицензияланган маҳсулотларни қўллашни мунтазам текшириш;

h) тегишли лицензион келишувлар шартларининг бажарилишини таъминлаш бўйича сиёсатни амалга ошириш;

i) дастурий таъминотни утилизация қилиш ёки бошқа ташкилотларга бериш қоидаларининг бажарилиши;

j) мунтазам аудитни ташкил қилиш;

k) умумий фойдаланиш тармоқларидан олинган дастурий таъминот ва ахборотга тегишли шартларни бажариш;

l) тижорат ёзувларини (фильмлар, аудио) муаллифлик ҳуқуқи тўғрисидаги қонунда рухсат этилганидан бошқача такрорлаш, бошқа форматга ўзгартириш ва улардан цитата келтиришни ман этиш;

m) китоблар, мақолалар, ҳисоботлар ёки бошқа ҳужжатлардан муаллифлик ҳуқуқи тўғрисидаги қонунда рухсат этилганидан бошқача тўлиқ ёки қисман нусха олишни ман этиш.

Бошқалар

Интеллектуал эгаликка ҳуқуқлар дастурий таъминотга ёки ҳужжатларга муаллифлик ҳуқуқларини, моделлар, савдо маркаларига, патентлар ва бошланғич кодларга лицензиялар учун бўлган ҳуқуқларини ўз ичига олади.

Кимнингдир эгалик предмети бўлган дастурий таъминот, одатда, муайян компьютерлар томонидан маҳсулотлардан фойдаланишни чеклайдиган лицензион келишув доирасида етказиб берилади, шунингдек, уларнинг резерв нусхаларини яратиш мақсадида улардан нусха кўчиришни чеклаши мумкин. Ходимларга ташкилот томонидан яратилган дастурий таъминот учун интеллектуал мулкка эгалик ҳуқуқлари билан боғлиқ вазиятни тушунтириш зарур.

Қонун ҳужжатлари, раҳбарий ҳужжатлар ва шартномаларнинг талаблари эгалик предмети ҳисобланган материаллардан нусха кўчиришни чеклаши мумкин. Хусусан, бу чеклашлар ташкилот томонидан ишлаб чиқилган ёки лицензияланган ёки ишлаб чиқувчи томонидан фақат ташкилот учун тақдим этиладиган материаллардан фойдаланиш

талабларини ўз ичига олиши мумкин. Муаллифлик ҳуқуқини бузиш жиноий жавобгарлик кўзда тутилган суд жараёнига олиб келиши мумкин.

15.1.3 Ташкилот ҳужжатларини муҳофаза қилиш

Бошқариш воситаси

Ташкилотнинг конфиденциал маълумотларини йўқолиш, бузилиш ва соҳталаштиришдан устав, қонун ҳужжатлари ва норматив ҳужжатлар, шартномалар ва бизнес талабларига мувофиқ муҳофаза қилиш керак.

Жорий этиш бўйича қўлланма

Маълумотларни турлари бўйича, масалан, бухгалтерлик ёзувлари, маълумотлар базаларининг ёзувлари, транзакциялар журналлари, аудит ва операцион ишлаш процедуралари журналлари, ҳар бирини сақлаш даври ва сақланадиган маълумотлар ташувчиларининг турлари, масалан, қоғоз, микрофильм, магнит ёки оптик тушувчилари кўрсатилган ҳолда таснифлаш керак. Ҳужжатларни сақлаш даври мобайнида шифрдан чиқариш имконини таъминлаш учун шифрланган архивлар ёки электрон рақамли имзолар билан боғлиқ ҳар қандай криптографик калитларни сақлаш керак. (12.3).

Маълумотларни сақлаш учун ишлатиладиган ташувчиларнинг сифатини пасайтириш имкониятини ҳисобга олиш керак. Маълумот ташувчиларини сақлаш ва уларга қараш бўйича процедураларни ишлаб чиқарувчининг тавсияларига мувофиқ амалга ошириш керак. Узоқ сақлаш учун қоғоздан ва микрофильмлардан фойдаланишни кўриб чиқиш керак.

Маълумотларнинг электрон ташувчиларидан фойдаланганда, ахборот технологиялардаги бўлғуси ўзгаришлар натижасида уларни йўқотишдан муҳофаза қилиш мақсадида уларни сақлаш даври мобайнида маълумотлардан фойдаланиш мумкинлигини текшириш (ташувчилар ва форматдаги маълумотларнинг ўқилиши) процедураларини қўллаш керак.

Маълумотларни сақлаш тизимини шундай танлаш керакки, талаб қилинган маълумотлар бажарилиши керак бўлган талабларга қараб мақбул вақт ичида ва мақбул форматда тикланиши мумкин бўлсин.

Сақлаш тизими маълумотларни аниқ идентификация қилинишини, шунингдек, қонун ҳужжатлари ва раҳбарий ҳужжатлар томонидан белгиланган сақлаш даврини таъминлаши зарур. Ушбу тизим ташкилотда маълумотларни сақлаш муддати тугаганида, маълумотлар керак бўлмай қолганда, уларни йўқ қилиш имкониятини тақдим этиши керак.

Ташкилот ҳужжатларини муҳофаза қилиш бўйича мақсадларга эришиш учун:

a) ахборотни сақлаш муддатлари ва тартибига, шунингдек, утилизация қилинишига тегишли қўлланмаларни ишлаб чиқиш;

b) энг муҳим маълумотларни сақлаш режа-жадвалини тузиш;

c) асосий ахборот манбаларининг рўйхатини юритиш;

d) конфиденциал ахборотни йўқотиш, бузиш ва соҳталаштиришдан муҳофаза қилиш учун тегишли чораларни жорий қилиш керак.

Бошқалар

Баъзи маълумотларга нисбатан қонун ҳужжатлари ва раҳбарий ҳужжатлар талабларини бажариш, шунингдек, конфиденциал бизнес-иловаларни қўллаб-қувватлаш мақсадида сақлаш хавфсизлигини таъминлаш талаб қилиниши мумкин. Мисол тариқасида ташкилот қонун ҳужжатлари ёки раҳбарий ҳужжатлар томонидан белгиланган нормалар доирасида ёки фуқаролик ёки жиноий жавобгарликдан адекват муҳофаза қилиш мақсадида, шунингдек, акционерлар, шериклар ва аудитлар учун ташкилотнинг молиявий аҳволини тасдиқлаш учун ишлашини исботлаш учун керак бўлиши мумкин бўлган маълумотларни келтириш мумкин. Маълумотларни сақлаш вақти ва маълумотлар мазмуни давлат қонун ҳужжатлари ва раҳбарий ҳужжатларига мувофиқ белгиланиши мумкин.

Ташкилот ҳужжатларини бошқариш тўғрисидаги батафсил ахборот ISO 15489-1 да берилган.

15.1.4 Маълумотларни муҳофаза қилиш ва шахсий ахборотнинг конфиденциаллиги

Бошқариш воситаси

Шахсий ахборот маълумотларининг муҳофазаси ва конфиденциаллиги тегишли қонун ҳужжатлари, нормалар ва жоиз бўлса, шартномалар бандларининг талабларига мувофиқ таъминланиши керак.

Жорий этиш бўйича қўлланма

Ташкилот шахсий ахбороти маълумотларининг муҳофазаси ва конфиденциаллигининг сиёсатини ишлаб чиқиш ва жорий этиш керак. Ушбу сиёсат шахсий ахборотга ишлов беришда қатнашадиган барча шахсларга етказилиши керак.

Ушбу сиёсатга риоя қилиш ва маълумотларни муҳофаза қилиш бўйича қонун ҳужжатларига мувофиқлик ахборот хавфсизлигини бошқаришнинг тегишли структурасини талаб қилади. Энг яхшиси бунга шахсий маълумотларни муҳофаза қилишга жавобгар шахсни тайинлашда менежерлар, фойдаланувчилар ва хизматларни етказиб берувчиларга уларнинг шахсан жавобгарлиги, шунингдек, тегишли тадбирларни бажариши мажбурийлиги тўғрисида тегишли равишда тушунтириш йўли билан эришилади. Шахсий ахборот билан ишлаш учун тегишли қонун ҳужжатлари, нормаларнинг барча талабларига риоя қилган ҳолда жавобгарлик билан ёндашиш керак. Шахсий ахборотни муҳофаза қилиш бўйича лозим бўлган техник ва ташкилий тадбирларни жорий этиш зарур.

Бошқалар

Бир қатор мамлакатларда шахсий мълумотларга ишлов бериш ва уларни узатишга тегишли чеклашлар белгиланган қонун ҳужжатларининг нормалари киритилган (бу асосан, ўша ахборот ёрдамида идентификация қилиниши мумкин бўлган жисмоний шахслар тўғрисидаги ахборотга тегишли). Бундай чеклашлар шахсий маълумотларни йиғиш, унга ишлов бериш, уни тарқатишни амалга оширувчиларга мажбуриятлар юклаши,

шунингдек, ушбу маълумотларни бошқа мамлакатларга узатиш имконини чеклаши мумкин.

15.1.5 Ахборотга ишлов бериш воситаларидан мақсадсиз фойдаланишнинг олдини олиш

Бошқариш воситаси

Фойдаланувчилар томонидан ахборотга ишлов бериш воситаларидан мақсадсиз фойдаланишга қаршилик кўрсатадиган чораларни татбиқ этиш зарур.

Жорий этиш бўйича қўлланма

Раҳбарият фойдаланувчиларнинг ахборотга ишлов бериш воситаларига тегишли ваколатлар даражаларини белгилаши керак. Ушбу воситалардан раҳбарият томонидан маъқулланмасдан (6.1.4) ишлаб чиқармайдиган ва рухсат берилмаган мақсадлар учун ҳар қандай фойдаланишни мақсадсиз деб баҳолаш керак. Агар ушбу фаолият мониторинг ёрдамида ёки қандайдир бошқа усуллар билан аниқланган бўлса, интизомий чоралар кўриш ва/ёки суд даъвосини инициация қилиш учун ходим бевосита раҳбарининг эътиборини тортиш керак.

Мониторинг бошлангунга қадар юрист маслаҳатини олиш керак.

Барча фойдаланувчилар уларга рухсат берилган фойдаланишнинг аниқ чегаралари ва рухсатсиз фойдаланишни аниқлаш бўйича мониторинг мавжудлиги тўғрисида хабардор бўлишлари керак. Бунга, масалан, фойдаланувчиларга нусхаси ташкилотда хавфсиз усулда сақланиши керак бўлган ёзма ваколатларга имзо қўйдириб уларга тақдим этиш йўли билан эришиш мумкин. Ташкилот ходимлари, субпудратчилар ва бегонга ташкилот фойдаланувчилари барча ҳолларда уларга фойдаланиш рухсат этилган маълумотлардан фойдаланиш ҳуқуқига эга эканликлари тўғрисида хабардор бўлишлари зарур.

Шунингдек, тизимдан фойдаланишни рўйхатдан ўтказиш вақтида компьютер экранида фойдаланувчилар киримоқчи бўлган тизим фойдаланиши чекланган тизим эканлигини ва ундан рухсатсиз фойдаланиш тақиқланганлигини кўрсатувчи, огоҳлантирувчи маълумот акс этиши зарур. Фойдаланувчи буни ўқиганлигини тасдиқлаши ва рўйхатга олиш жараёнини давом эттириш учун унга тегишли равишда жавоб бериши керак (11.5.1).

Бошқалар

Ахборотга ишлов бериш воситалари фақат ишга оид мақсадлар учун мўлжалланган.

Бузиб киришларни аниқлаш, ичидагини назорат қилиш ва бошқа кузатиб бориш асбоблари ахборотга ишлов бериш воситаларидан рухсатсиз фойдаланишнинг олдини олишга ёрдам бериши мумкин.

Кўпгина мамлакатларда компьютердан ўз манфаати учун фойдаланишдан муҳофаза қилиш бўйича қонун ҳужжатлари бор. Компьютердан рухсат берилмаган мақсадлар учун фойдаланиш жиноят ҳисобланиши мумкин.

Мониторингдан фойдаланишнинг қонунийлиги мамлакатда амалда бўлган қонун ҳужжатларига боғлиқ. Мониторинг ўтказилиши тўғрисида ходимлар хабардор бўлишлари ва уни ўтказиш учун уларнинг ҳужжатлаштирилган розиликларини олиш керак бўлиб қолиши мумкин. Агар фойдаланувчи кирадиган тизим умумий фойдаланиш учун қўлланса (масалан, умумий веб-сервер) ва хавфсизликни кузатиб боришга мансуб бўлса, тегишли хабар кўрсатилган бўлиши керак.

15.1.6 Муҳофаза қилишнинг криптографик воситаларидан фойдаланишни тартибга солиш

Бошқариш воситаси

Ахборотни муҳофаза қилишнинг криптографик воситаларидан қонун ҳужжатлари талаблари ва норматив талабларга мувофиқ фойдаланиш керак.

Жорий этиш бўйича қўлланма

Тегишли қонун ҳужжатлари талаблари ва норматив талабларга риоя қилиш учун қуйидагиларни ҳисобга олиш зарур:

a) криптографик функцияларни бажарувчи компьютер аппарат таъминоти ва дастурий таъминот импорти ва/ёки экспорти учун чеклашлар;

b) қўшимча криптографик функцияларни қўшиш мумкин бўлган аппарат таъминоти ва дастурий таъминот импорти ва/ёки экспорти учун чеклашлар;

c) шифрлашдан фойдаланишга чеклашлар;

d) ахборот мазмунининг кофиденциаллигини таъминлаш учун аппарат ва дастурий воситалар ёрдамида шифрланган ахборотга давлат томонидан фойдаланишнинг мажбурий ёки дискрецион методлари.

Ташкилотда криптографик воситалардан фойдаланиш сиёсати миллий қонун ҳужжатларига мувофиқлигига ишонч ҳосил қилиш учун юристнинг маслаҳати зарур. Шифрланган ахборот ёки криптографик восита бошқа давлатга юборилишидан олдин юристнинг маслаҳатини олиш зарур.

15.2 Хавфсизлик сиёсати ва стандартлар талабларига мувофиқлик

Мақсад: ахборот тизимлари ташкилотнинг хавфсизлик сиёсатига ва стандартларга мувофиқлигини таъминлаш.

Ахборот тизимларининг хавфсизлигини мунтазам таҳлил қилиш ва баҳолаш зарур.

Ушбу текширувларни хавфсизликнинг тегишли сиёсатлари ва техник платформалари борасида амалга ошириш зарур, дастурий воситалар ва ахборот тизимлари эса, ушбу сиёсатларга ва рўйхатдан ўтказилган хавфсизликни бошқариш воситаларига мувофиқлигининг аудити ўтказилиши керак.

15.2.1 Хавфсизлик сиёсатига ва стандартларга мувофиқлик

Бошқариш воситаси

Хавфсизлик сиёсатига ва стандартларга мувофиқликка эришиш учун раҳбарлар ўзларининг жавобгарлик доираларида барча хавфсизлик процедуралари тўғри бажарилишини таъминлашлари керак.

Жорий этиш бўйича қўлланма

Раҳбарлар ўзларининг жавобгарлик доираларида тегишли хавфсизлик сиёсатига ва стандартларга, шунингдек, ахборотга ишлов беришда хавфсизликнинг бошқа талабларига риоя қилинишини мунтазам текширишлари керак.

Агар текширув натижасида номувофиқлик аниқланса, у ҳолда раҳбарлар қўйидагиларни бажариши керак:

a) номувофиқликнинг сабабларини аниқлаш;

b) номувофиқликнинг такрорланишига йўл қўймайдиган тадбирларга бўлган эҳтиёжни баҳолаш;

c) киритилиши лозим бўлган тузатишларни аниқлаш ва амалга ошириш;

d) қўлланган тузатувчи таъсирни текшириш.

Раҳбарлар томонидан бажариладиган текширувлар ва тузатувчи таъсирларнинг натижаларини ёзиб бориш, ёзувлар маълумотларини эса, сақлаш керак. Мустақил текширув ушбу раҳбарларнинг жавобгарлик доирасига ўтганда, раҳбарлар текширувлар натижалари тўғрисида мустақил текширувлар ўтказадиган шахсларга (6.1.8) хабар беришлари керак.

Бошқалар

Ахборот тизимларидан фойдаланишни эксплуатацион кузатиб бориш мумкинлиги 10.10-бандда таърифланган.

15.2.2 Техник мувофиқликни текшириш

Бошқариш воситаси

Ахборот тизимларининг ахборот хавфсизлиги соҳасидаги стандартларга мувофиқлигини мунтазам текшириш керак.

Жорий этиш бўйича қўлланма

Техник мувофиқликни текширишни тажрибали тизим муҳандиси қўлда (зарур бўлганда, тегишли инструментал ва дастурий воситалар ёрдамида) ёки техник ҳисоботни техник мутахассис томонидан кейинчалик таҳлил қилиш учун генерация қиладиган дастурларнинг автоматлаштирилган пакети ёрдамида амалга ошириш керак.

Агар кириб олиш ёки заифликни баҳолаш учун текшириш қўлланса, эҳтиёткорликка риоя қилиш керак, чунки бундай амаллар тизим хавфсизлигининг бузилишига олиб келиши мумкин. Бундай текширувларни режалаштириш, ҳужжатлаштириш ва такрорлаш керак.

Хавфсизлик талабларига мувофиқликнинг ҳар қандай текшируви фақат ваколатли, авторизация қилинган шахслар томонидан ёхуд уларнинг кузатуви остида бажарилиши керак.

Бошқалар

Техник мувофиқликни текшириш бошқаришнинг аппарат ва дастурий воситаларини тўғри жорий этилишини таъминлаш учун амалдаги тизимларни кўздан кечиршни ўз ичига олади. Текширувнинг бу тури ихтисослаштирилган техник экспертизани талаб қилади.

Техник мувофиқликни текшириш, шунингдек, атайлаб ушбу мақсад учун таклиф қилинган мустақил экспертлар томонидан бажарилиши мумкин бўлган текширувни, масалан кириб олиш ва заифликларни баҳолашни ўз ичига олади. Бу тизимдаги заифликларни аниқлаш ва ушбу заифлик туфайли рухсатсиз фойдаланишни бошқариш воситалари ёрдамида олдини олишнинг самарадорлилигини текшириш учун фойдали бўлиши мумкин.

Кириб олиш ва заифликларни баҳолашни текшириш тизимнинг муайян вақт ичида, муайян ҳолатдаги бир лаҳзалик суратини таъминлайди. Ушбу сурат кириб олишга уриниш(лар)да тизимнинг ҳақиқатда текширилган қисмлари томонидан чегараланган. Кириб олиш ва заифликларни баҳолашни текшириш заифликларни аниқлашнинг ўрнини босмайди.

15.3 Ахборот тизимларининг аудит масалалари

Мақсад: ахборот тизими аудитининг максимал самарадорлилигини ва унинг ахборот хавфсизлигига минимал таъсирини таъминлаш.

Тизимларнинг аудитини ўтказиш жараёнида ишчи муҳит ва аудит инструментал воситаларининг ахборот хавфсизлигини таъминлаш бўйича тадбирларни кўзда тутиш зарур.

Шунингдек, ахборот тизимининг бутлигини таъминлаш ва аудит инструментал воситаларидан нотўғри фойдаланишнинг олдини олиш учун муҳофаза талаб қилинади.

15.3.1 Ахборот тизимларининг аудитини бошқариш

Бошқариш воситаси

Бизнес-жараёнлар учун хавфни минимумга келтириш учун операцион тизимларнинг текширувини ўз ичига олган аудит талаблари ва амалларини пухта режалаштириш ва келишиш керак.

Жорий этиш бўйича қўлланма

Қуйидагиларни ҳисобга олиш керак:

a) аудит талабларини тегишли раҳбарлар билан келишиш керак;

b) текширувлар ҳажмини келишиш ва назорат қилиш керак;

c) текширувлар дастурий таъминотдан ва фақат ўқиш учун маълумотлардан фойдаланиш билан чекланиши керак;

d) фақат ўқиш учун фойдаланишдан фарқли фойдаланишни аудит тугаганидан сўнг йўқ қилиниши ёки агар аудит ҳужжатларининг талабларига мувофиқ бундай файлларни сақлаб қўйиш зарурати бўлса,

лозим даражада муҳофаза қилиниши керак бўлган тизим файлларининг ажратилган нусхалари учун рухсат берилиши керак;

e) текширувларни ўтказиш учун ахборот тизимларининг зарур активларини аниқ идентификация қилиш ва улардан фойдаланишни таъминлаш зарур;

f) маълумотларга махсус ёки қўшимча ишлов беришга қўйилган талабларни идентификация қилиш ва келишиш керак;

g) кейинги ҳаволалар учун баённома тузиш мақсадида барча фойдаланишнинг мониторинги ўтказилиши ва рўйхатга олиниши керак;

h) аудитнинг барча процедуралари, талаблари ва мажбуриятлари ҳужжатлаштирилиши керак;

i) аудитни бажарувчи шахс (шахслар) аудит жараёнларига боғлиқ бўлмаслиги (ликлари) керак.

15.3.2 Ахборот тизимлари аудитининг инструментал воситаларини муҳофаза қилиш

Бошқариш воситаси

Ҳар қандай мумкин бўлган нотўғри фойдаланиш ёки уларни компрометация қилишнинг олдини олиш учун аудитнинг инструментал воситаларидан, яъни дастурий таъминот ёки маълумотлар файлларидан фойдаланишни муҳофаза қилиш зарур.

Жорий этиш бўйича қўлланма

Ахборот тизимлари аудитининг инструментал воситаларини, масалан, дастурий таъминот ёки маълумотлар файлларини ишлаб чиқиш тизимлари ва амалдаги тизимлардан ажратиш керак ва қўшимча муҳофазанинг тегишли даражаси таъминланмаган бўлса, кутубхоналардаги ташувчиларда ёки фойдаланувчининг соҳаларида сақламаслик керак.

Бошқалар

Агар аудитда учинчи шахслар жалб этилган бўлса, ушбу шахслар томонидан аудитнинг инструментал воситаларидан ғайриқонуний фойдаланиш ва ташкилот ахборотидан фойдаланиш хавфи бор. Ушбу хавфни ҳисобга олиш учун хавфларни аниқлаш (6.2.1) ва жисмоний фойдаланшни чеклаш (9.1.2) каби бошқариш воситаларини кўриб чиқиш, шунингдек, кейинги амалларни, масалан, аудиторларга маълум бўлган паролларни дарҳол ўзгартириш амалларини қўллаш керак.

Библиография

ISO/IEC Guide 2:1996, Standardization and related activities - General vocabulary (ISO/IEC, Руководство 2:1996, Стандартизация и связанная с ней деятельность - Общий словарь).

ISO/IEC Guide 73:2002, Risk management - Vocabulary - Guidelines for use in standards (ISO/IEC, Руководство 73:2002, Управление рисками - Словарь - Рекомендации по использованию в стандартах).

ISO/IEC 13335-1:2004, Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management (ISO/IEC 13335-1:2004, Информационные технологии - Методики безопасности - Управление безопасностью информационных и коммуникационных технологий - Часть 1: Концепции и модели управления безопасностью информационных и коммуникационных технологий).

ISO/IEC TR 13335-3:1998, Information technology - Guidelines for the Management of IT Security - Part 3: Techniques for the management of IT Security (ISO/IEC TR 13335-3:1998, Информационные технологии - Рекомендации по управлению безопасностью информационных технологий - Часть 3: Методики управления безопасностью информационных технологий).

ISO/IEC 13888-1: 1997, Information technology - Security techniques - Non-repudiation - Part 1: General (ISO/IEC 13888-1: 1997, Информационные технологии - Методики безопасности - Апеллируемость - Часть 1: Общие положения)

ISO/IEC 11770-1:1996 Information technology - Security techniques - Key management - Part 1: Framework (ISO/IEC 11770-1:1996 Информационные технологии - Методики безопасности - Управление ключами - Часть 1: Структурная основа).

ISO/IEC 9796-2:2002 Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms (ISO/IEC 9796-2:2002 Информационные технологии - Методики безопасности - Схемы цифровых подписей, обеспечивающие восстановление сообщений - Часть 2: Механизмы, основанные на разложении целых чисел на множители).

ISO/IEC 9796-3:2000 Information technology - Security techniques - Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms (ISO/IEC 9796-3:2000 Информационные технологии - Методики безопасности - Схемы цифровых подписей, обеспечивающие восстановление сообщений - Часть 3: Механизмы, основанные на дискретных логарифмах).

ISO/IEC 14888-1:1998 Information technology - Security techniques - Digital signatures with appendix - Part 1: General (ISO/IEC 14888-1:1998

Информационные технологии - Методики безопасности - Цифровые подписи с приложением - Часть 1: Общие положения).

O‘z DSt ISO/IEC 15408-1:2008 Information technology - Security techniques - Evaluation Criteria for IT security - Part 1: Introduction and general model (O‘z DSt ISO/IEC 15408-1:2008 Информационные технологии - Методики безопасности - Критерии оценки безопасности информационных технологий - Часть 1: Введение и общая модель).

ISO/IEC 14516:2002 Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services (ISO/IEC 14516:2002 Информационные технологии - Методики безопасности - Рекомендации по использованию и управлению услугами Доверенных третьих сторон).

ISO 15489-1:2001 Information and documentation - Records management - Part 1: General (ISO 15489-1:2001 Информация и документация - Управление документами - Часть 1: Общие положения).

ISO 10007:2003 Quality management systems - Guidelines for configuration management (ISO 10007:2003 Системы управления качеством - Рекомендации по управлению конфигурациями).

ISO/IEC 12207:1995 Information technology - Software life cycle processes (ISO/IEC 12207:1995 Информационные технологии - Процессы жизненного цикла программного обеспечения).

ISO 19011:2002 Guidelines for quality and /or environmental management systems auditing (ISO 19011:2002 Рекомендации по аудиту систем управления качеством и/или средой).

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security', 2002 (OECD Рекомендации по безопасности информационных систем и сетей: 'Навстречу культуре безопасности', 2002)

OECD Guidelines for Cryptography Policy, 1997 (OECD Рекомендации по криптографической политике, 1997).

IEEE P1363-2000: Standard Specifications for Public-Key Cryptography (IEEE PI363-2000: Стандартные спецификации по криптографии с открытыми ключами).

ISO/IEC 18028-4 Information technology - Security techniques - IT Network security -Part 4: Securing remote access (ISO/IEC 18028-4 Информационные технологии -Методики безопасности - Безопасность информационных сетей - Часть 4: Защита удаленного доступа).

ISO/IEC TR 18044 Information technology - Security techniques - Information security incident management (ISO/IEC TR 18044 Информационные технологии - Методики безопасности - Управление инцидентами информационной безопасности).

УЎТ СУТ 35.040

Асосий сўзлар: хавфларни аниқлаш, ташкилот, амалий қоидалар, ахборот хавфсизлиги, ахборот хавфсизлиги сиёсати, фойдаланишни бошқариш, хавфларни бошқариш.